# FortiAuthenticator™ FSSO Authentication

User Guide

FortiAuthenticator™ FSSO Authentication User Guide

October 20, 2014

Revision 4



| | |
|---|---|
| Technical Documentation | http://help.fortinet.com |
| Knowledge Base | http://kb.fortinet.com |
| Forums | https://support.fortinet.com/forums |
| Customer Service & Support | https://support.fortinet.com |
| Training | http://training.fortinet.com |
| FortiGuard Threat Research & Response | http://www.fortiguard.com |
| License Agreement | http://www.fortinet.com/doc/legal/EULA.pdf |
| Document Feedback | Email: techdocs@fortinet.com |

# Table of contents

# Change Log

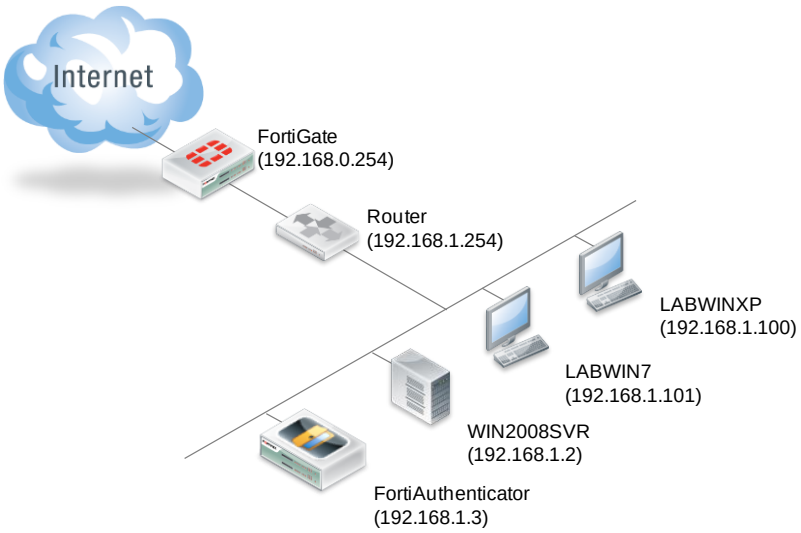
| Revision | Date | Change Description |
|---|---|---|
| 1 | 2012-11-05 | Initial Release |
| 2 | 2012-12-05 | Updated to include RADIUS to FSSO Authentication |
| 3 | 2013-09-27 | Updated to reflect changes in version 3.0 |
| 4 | 2014-07-09 | Updated to reflect changes in version 3.1 |
| 5 | 2014-07-16 | Updated with additional Kerberos debugging |
| 6 | 2014-10-20 | Updated to reflect changes in version 3.2<br>Corrected redirect URLs to reflect recent FortiOS changes |

# Introduction

This document introduces the FortiAuthenticator FSSO Authentication Methods and how they can be configured for use in a FortiGate environment. The document covers the configuration of the FortiAuthenticator, Active Directory, and FortiGate.

## Lab Setup

For this lab, a simple setup, as shown below was used. This configuration is applicable to most common deployment scenarios including corporate LAN deployments.




## Software versions

The configuration discussed in this document was tested on the following firmware versions:

FortiAuthenticator 3.1

FortiGate 5.0 GA PR7

FortiClient 5.0

Windows 2008 Server R2 (x64)

Windows XP SP3 (x86)

Windows 7 SP1 (x64)

# FortiAuthenticator FSSO Authentication

Fortinet Single Sign-On (FSSO) is a general term used by Fortinet to describe methods to transparently authenticate users, commonly but not limited to Active Directory users, on to a FortiGate device so that Identity Based Policies (IBP) can be applied.

## Identity Based Policies

Identity Based Policies are how FortiOS uses user identity provided by FSSO to deliver comprehensive user identity centric security. Instead of allowing access based on physical location or IP address, Identity Based Policies enable access to resources based on who the user is and what their role is within an organization.

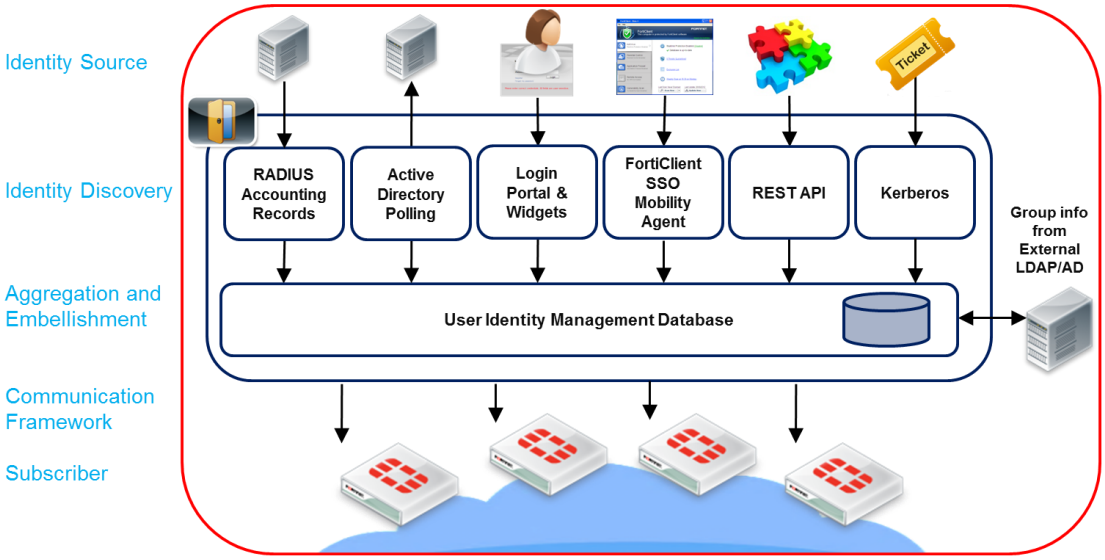

## The FortiAuthenticator FSSO Framework

FSSO has existed alongside FortiGate devices for several years the form of agents which collect user identity information by querying security event logs either by polling or on an active directory domain controller.

In effect, FSSO is a communications framework to pass user identity information to FortiGate or FortiCache devices, however the method of gathering authentication events is flexible. FortiAuthenticator has taken this premise and enhanced the solution with additional authentication methods which can be used to populate the FSSO user identity database.

FortiAuthenticator integrates with commonly used directory services and standards to improve the user experience by reducing the number of authentication requests required to gain access to network resources.

There are five layers within the FortiAuthenticator SSO framework:




**Identity Source** The method by which the user identity is ascertained.

**Discovery Methods:** Methods in which the user identity and their location (IP) are discovered.

**Aggregation and Embellishment:** Collection of user identity and addition of any missing information (e.g. group)

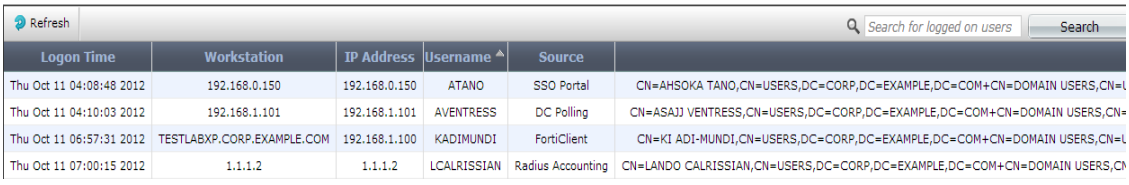
**Communication Framework:** Method by which the authentication information is communicated with the subscribing device

**Subscriber:** Device that subscribes to the FortiAuthenticator FSSO feed, commonly to use in Identity Based Policy.

O

Once identified using one of these methods, user information is communicated to the FortiAuthenticator where it can be embellished with additional information e.g. Group membership taken from LDAP or Active Directory and forwarded selectively to FortiGate or FortiCache devices where the information can be utilized in dynamic Identity Based Policies.

Multiple methods can be combined to deliver the greatest possible coverage of clients and user experience for example Single Sign On Mobility Agent may be used for Microsoft Windows domain PCs but fallback to the login portal with embedded widgets for non-windows systems or unauthenticated PCs. Such a system utilizing multiple authentication methods is shown below.


Refresh

Search for logged on users | Search

| Logon Time | Workstation | IP Address | Username | Source | |
|---|---|---|---|---|---|
| Thu Oct 11 04:08:48 2012 | 192.168.0.150 | 192.168.0.150 | ATANO | SSO Portal | CN=AHSOKA TANO,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM+CN=DOMAIN USERS,CN=U |
| Thu Oct 11 04:10:03 2012 | 192.168.1.101 | 192.168.1.101 | AVENTRESS | DC Polling | CN=ASAJJ VENTRESS,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM+CN=DOMAIN USERS,CN= |
| Thu Oct 11 06:57:31 2012 | TESTLABXP.CORP.EXAMPLE.COM | 192.168.1.100 | KADIMUNDI | FortiClient | CN=KI ADI-MUNDI,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM+CN=DOMAIN USERS,CN=U |
| Thu Oct 11 07:00:15 2012 | 1.1.1.2 | 1.1.1.2 | LCALRISSIAN | Radius Accounting | CN=LANDO CALRISSIAN,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM+CN=DOMAIN USERS,CN |

Note that this document only covers FSSO and whilst it covers RADIUS as a source of identity into FSSO, it does not does not discuss the use of RADIUS as a communication protocol into FortiGate/FortiMail, more commonly known as RSSO. This topic will be covered in the *RADIUS Proxy User Guide* http://docs.fortinet.com/fortiauthenticator/admin-guides.

## User Identity Discovery Methods

FortiAuthenticator has taken the concept of Fortinet Single Sign-On (FSSO) as used in FortiGate and the FSSO Software client and extended it with several new user identification methods. Due to the flexibility of the FortiAuthenticator product, this list is continuously growing. Current authentication sources and the user experiences provided are summarized below and configuration of these methods will described in more detail in Configuring FSSO Authentication.

### FSSO Domain Controller Polling

FortiAuthenticator is able to poll Windows Domain controllers to monitor the security event logs for login events. Polling of the Security Event Log is configured to occur every 5 seconds so that any login event that has occurred since the previous poll is captured and entered into FSSO.

Note that login events can be detected from the security event logs, logout cannot be detected. This is due to the fact that logout events can be triggered by many different processes e.g. closing of a windows share, however this is not indicative of the user logging out. To detect logout with DC Polling, additional methods need to be employed such as login timeouts or WMI Polling.

### Kerberos Authentication

To avoid the need to poll the domain controller whilst still retaining the ability to transparently authenticate Windows users, FortiAuthenticator supports use of Kerberos tickets passed by the browser and validated against the KDC to identify users.

### FortiClient Single Sign-On Mobility Agent

The FortiClient SSO Mobility Agent is part of the standard FortiClient product installation and can be installed on Windows XP/7/8 as part of the full FortiClient installation or, using the customized install process installed as a standalone component.

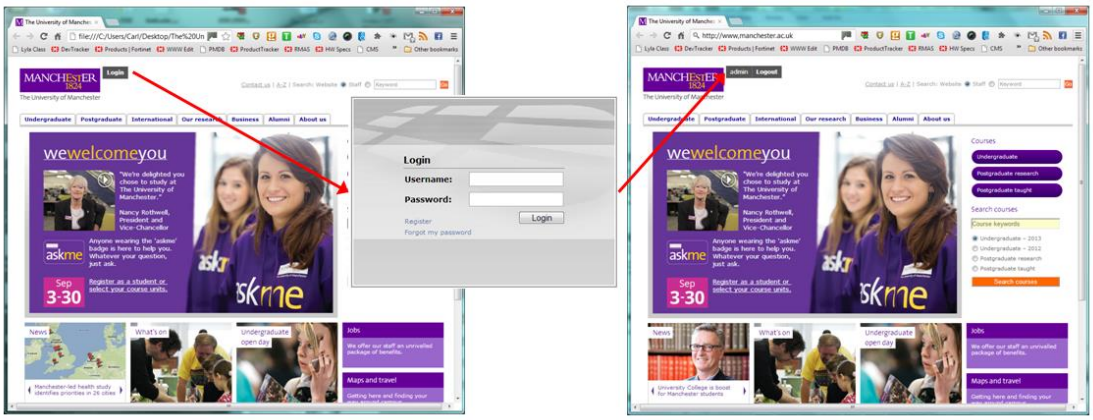
When installed, SSO Mobility Agent identifies Windows Domain users transparently and communicates the user identity and IP address to FortiAuthenticator for use in FSSO. The agent also monitors the system for IP address changes, such as those due to WiFi roaming, and automatically updates FortiAuthenticator. When the user logs off or shuts down, the user is also logged off from the FortiAuthenticator. In cases where an unclean disconnection is made (e.g. power failure, hibernation, network failure), a heartbeat system is implemented so the user will be de-authenticated following a configurable number of heartbeat failures.

### FSSO Portal Authentication

In situations where device or user identity cannot be established transparently, such as non-domain BYOD devices or shared kiosk machines, a web portal can be used to prompt users for login. This method is commonly combined with other transparent methods and used as a “catch-all” for non-domain and systems which cannot be identified transparently. Once authenticated, the user remains authenticated until they logoff from the browser.

As repeated manual re-authentication may impact the user experience, FortiAuthenticator supports automated user identification for subsequent accesses through the use of Portal Widgets. The Widget implementation, which uses a HTML iframe, can be incorporated into a web page, such as an intranet webpage for users to use for login. Following a successful login, a time limited cookie, validity of which is configurable for up to 30 days, is stored in the users browser. On subsequent to the users intranet home page, the user will be transparently re-authenticated using the cookie key (assuming it matches that stored on the

FortiAuthenticator). On timeout of the cookie, should the user clear their cache or visit a new machine, the user will be required to re-authenticate.




## Radius Accounting

The RADIUS accounting method uses RADIUS start, interim and stop accounting packets to trigger logon/logoff to FSSO. Such RADIUS packets are commonly sent by networking devices such as wireless controllers, switches and SSL-VPN devices amongst others.

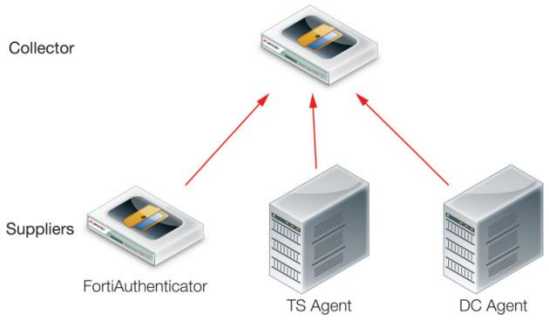
The benefit of this method is that for vendors who support sending such packets, no direct support is required by FortiAuthenticator (they use standard RADIUS which is already supported) and minimal change is required to enable the input of the user authentication data into the FSSO.

## FortiAuthenticator API

To enable integration with third party systems, FortiAuthenticator offers a programmatic REST API which can be used to authenticate and de-authenticate users into FSSO. This can be used for integration with third party applications such as portals and identity management systems. The API will not be covered in depth, for more details in the *FortiAuthenticator REST API Solution* Guide http://docs.fortinet.com/fortiauthenticator/admin-guides.

## Domain Controller and Terminal Services Agents

FortiGate devices support the concept of DCAgent software for the collection of login information from Windows Active Directory systems through either polling or installation on the domain controller. TSAgent is a similar concept, except it collects user login information from Citrix or Windows Terminal Servers. FortiAuthenticator implements the polling functionality directly; however, it also accepts a feed from both DCAgent and TSAgent installations if necessary.

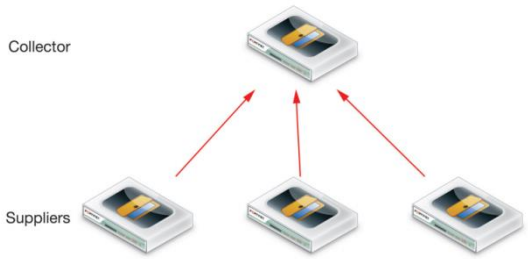


## Logout Detection

Whilst some methods natively support logout detection (e.g. SSO Mobility Agent), other such as AD polling do not. To enable logout detection, FortiAuthenticator supports WMI polling to identify the current logged in user state for a device and log the user out. A manual timeout period can also be set to remove the user form the authorization table after e.g. 8 hours.

## Hierarchical Tiering of Multiple FortiAuthenticator Devices

Tiering of collectors and suppliers allows for the large scale deployment of regional systems performing detection of user identification. It also allows local LDAP group lookup and distribution of events to top level collectors, which then distribute login events to FortiGate and FortiCache devices.



# Basic FSSO Configuration

This chapter documents the basic configuration required to enable Fortinet Single Sign on between the FortiAuthenticator and on the FortiGate. For details of how to configure the individual discovery methods, see the relevant chapters e.g.

Active Directory DC Polling

FortiClient Single Sign-On Mobility Agent

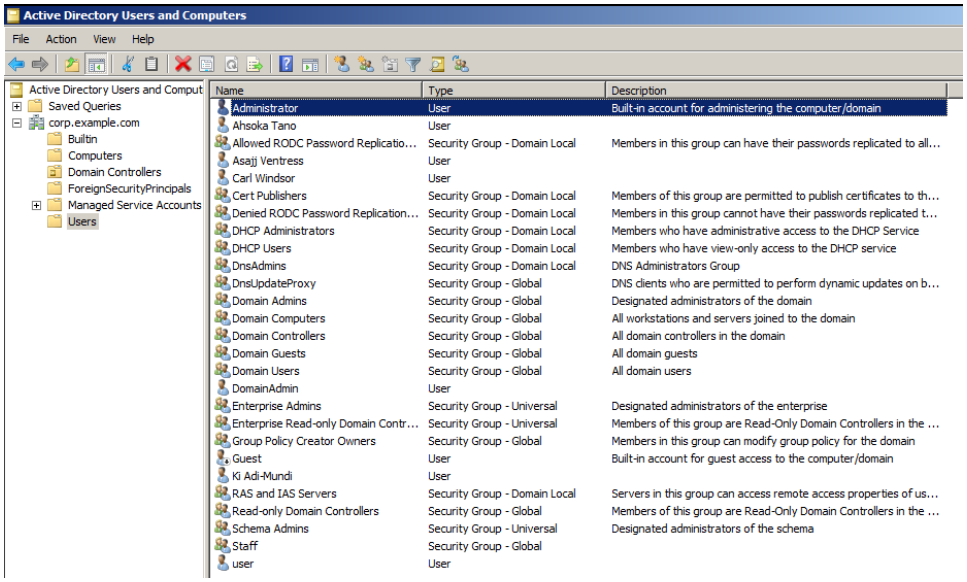
Portal Authentication

Radius Accounting

FortiAuthenticator API

## Configure the Windows Test Domain

For the purpose of this lab, a simple Windows 2008 domain was configured with the following schema:




The Base DN for the purpose of this lab can be seen as corp.example.com.

Several test users and a Security Group called Staff were created to verify the correct user and group membership could be passed to the FortiGate.

## Configure FortiAuthenticator AD (LDAP) connection

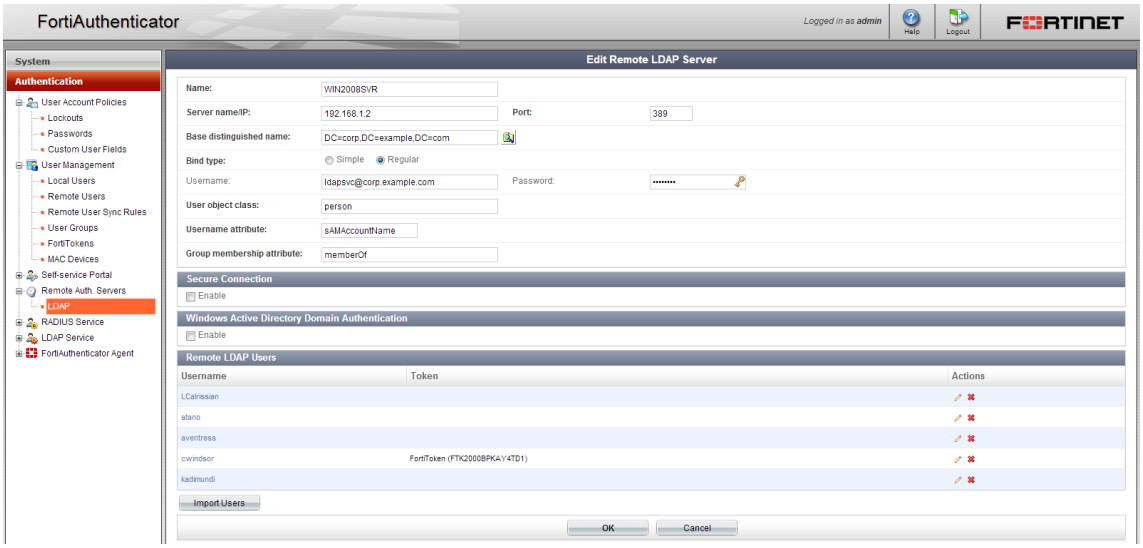
Browse to *Authentication → Remote Auth Servers →LDAP* and select ***New***.

In the resulting form, enter the details of the domain and the required credentials for authentication

- The Base DN should be entered as DC=corp,DC=example,DC=com
- The Bind type should be set to regular

- The user DN used to bind to the directory should a user with permissions to read the security event log specified as <USER>@<DOMAIN> e.g. ldapsvc@corp.example.com. See Appendix A – Domain Account Permissions for permissions required for this account.
-

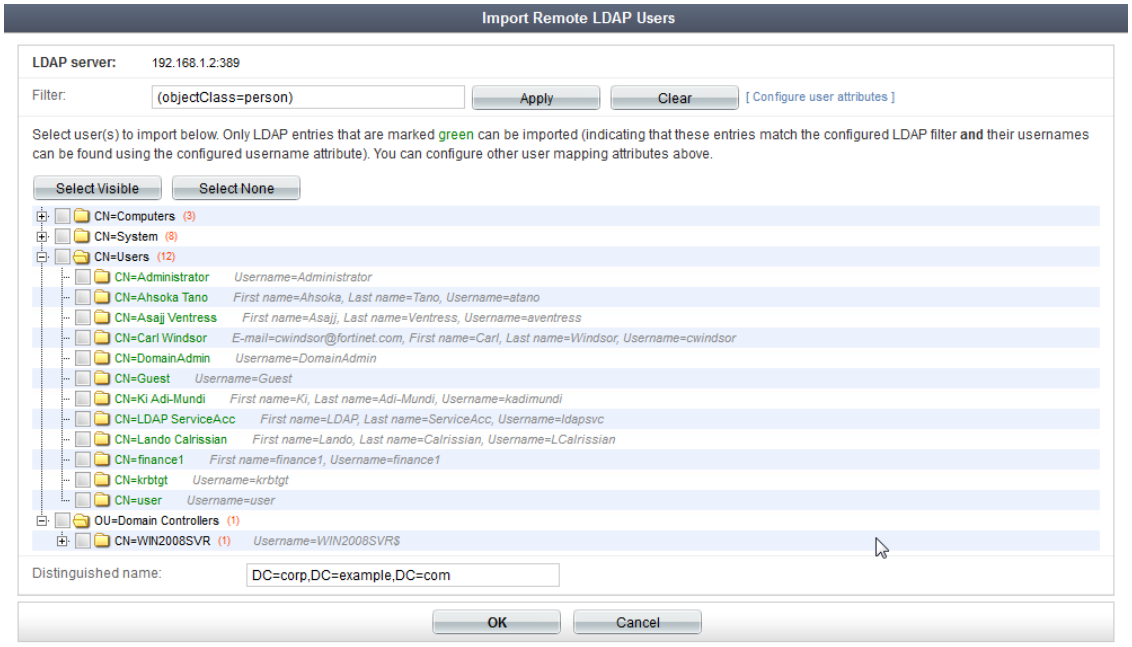
**Caution**. The user DN can be found using the Windows command *dsquery –name <USER>* and specified in the alternative format *CN=ldapsvc,DC=corp,DC=example,DC=com* . This entry format will appear to be successful and the admin will be able to browse the directory, even import users. However it is recommended that this format is not used as it can cause a later step to fail.




Ensure that the correct User object class, Username Attribute and Group Member Attributes are set for your specific LDAP directory. The defaults (shown) are for a default installation of Active directory. These values may need to be changed if using alternative LDAP systems.

Click Import users to verify that the directory can be accessed however, it is not necessary to actually import users. Importing users into the Remote Users database is only required for explicit authentication and two-factor authentication and not FSSO.

A successful connection to the directory should pull back the available containers and user list.



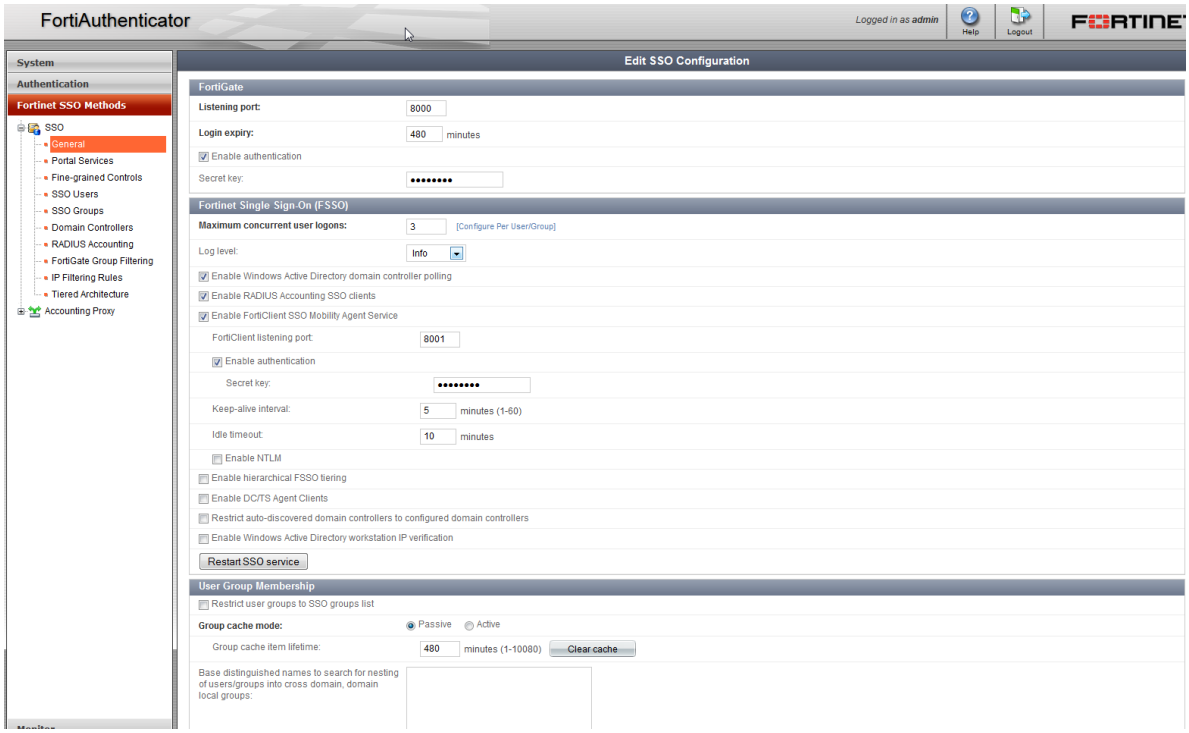

## Configure FortiGate FSSO communication

For FortiGate to accept FSSO user identity information, both the FortiAuthenticator and the FortiGate must be configured with the correct shared settings. This sections details the basic configuration required to get this working.

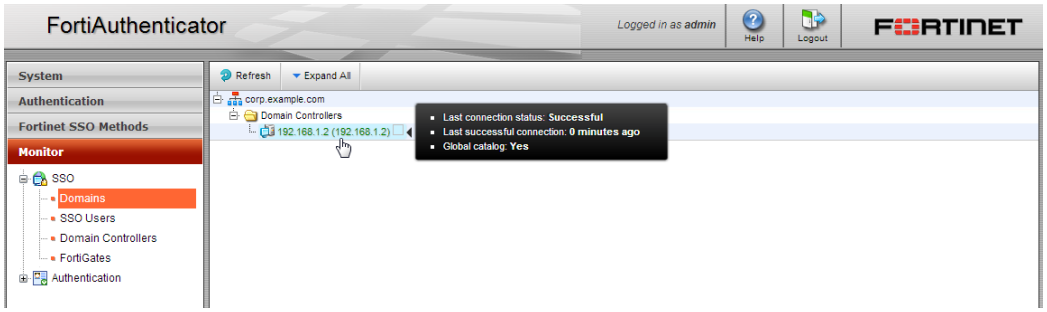
### FortiAuthenticator configuration

Browse to *Fortinet SSO Methods → SSO → General → FortiGate* configure the required listening port for the FortiGate (***default: 8000***) and create a secure secret key which will also need to be configured on the FortiGate.

Under *Fortinet SSO Methods → SSO → General → Fortinet Single Sign-On (FSSO), enable one of the methods e.g. 'Enable Active Directory Domain Controller Polling'*. FortiAuthenticator will start the FSSO process as soon as an SSO method is enabled.




Browsing to *Monitor → SSO → Domains* should provide visibility of the configured domain controller and any others discovered within the same domain.




## FortiGate configuration

The configuration provided demonstrates how to retrieve the login events from the remote FortiAuthenticator, it does not provide detail on how to apply the user and group information into an Identity Based Policy. See the FortiGate Authentication Guide for more information on how this can be achieved http://docs.fortinet.com/fgt.html.

Log into the FortiGate as an administrator and:

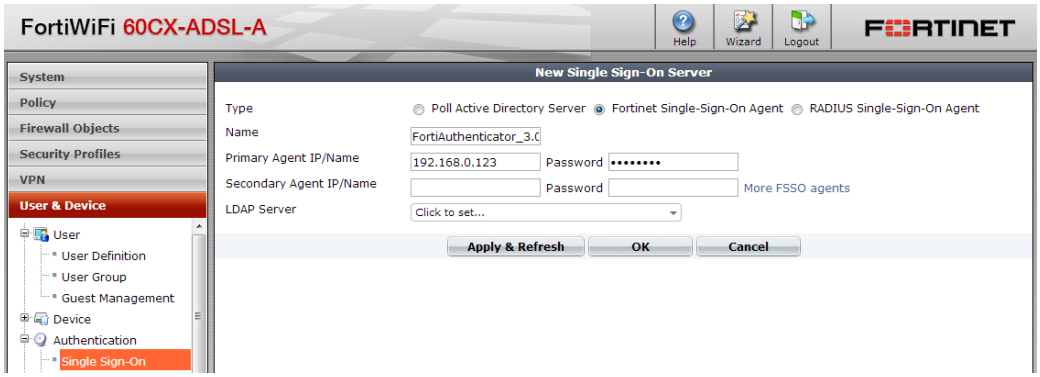
Browse to *User & Device → Authentication → Single Sign On* and select *Create New*.

Select Type: ***Fortinet Single Sign-On Agent***

Provide a descriptive *name* for the connections e.g. *FortiAuthenticator_3.0*.

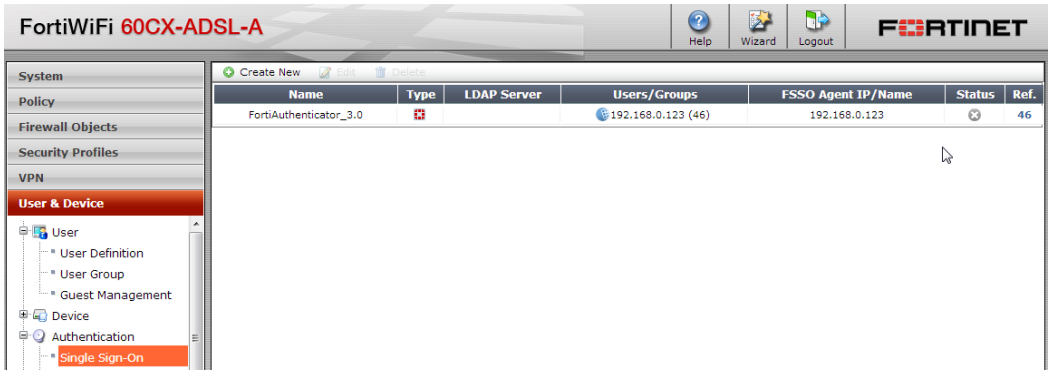
Enter the *Primary Agent IP* (that of the FortiAuthenticator) e.g. *192.168.0.123* and the password set on the FortiAuthenticator e.g. fortinet1234 then click ***OK***.

An LDAP server is not required as FortiAuthenticator will collect the group information from LDAP.



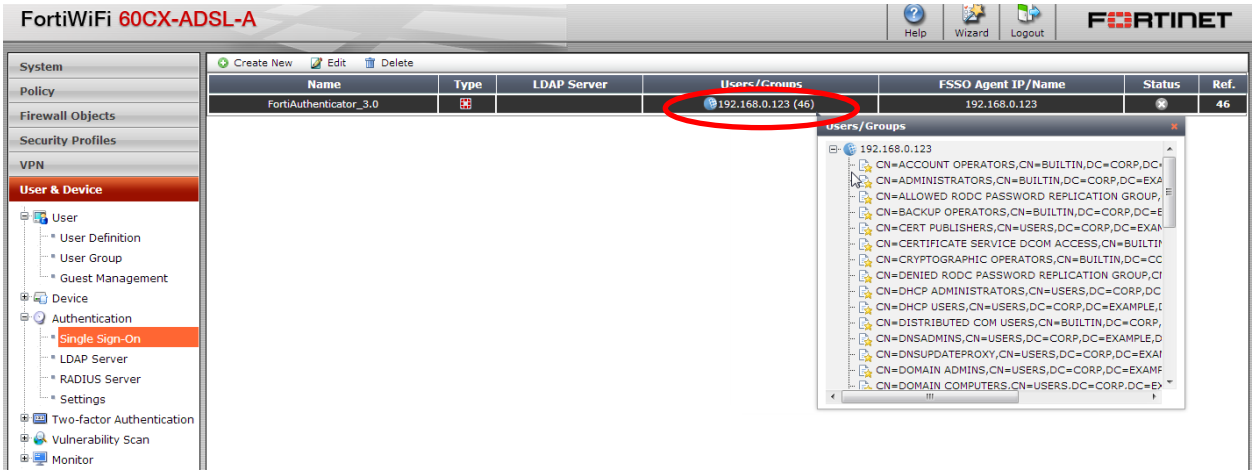

Once the connection has been created, the connection status should show up as a green tick under *User & Device → Authentication → Single Sign-On*.

**Note:** In the screenshot below taken form FortiOS 5.0.4, the FSSO status is showing as disconnected, however functions correctly. This is a known cosmetic issue and will be remedied in a future FortiGate release.

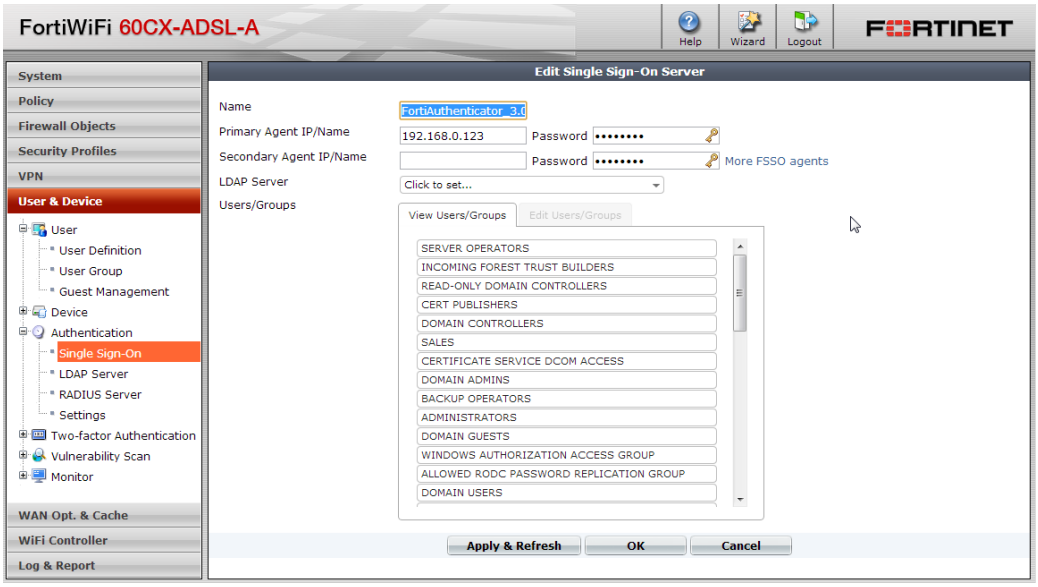



After a few minutes, the FortiGate should have pulled down the list of available groups on the FortiAuthenticator. This includes the remote groups available to it from the remote AD system(s). This is indicated by the number of groups shown in parenthesis as indicated below (46).

Click on the *User/Groups* entry for that server to display the Group list that has been retrieved,

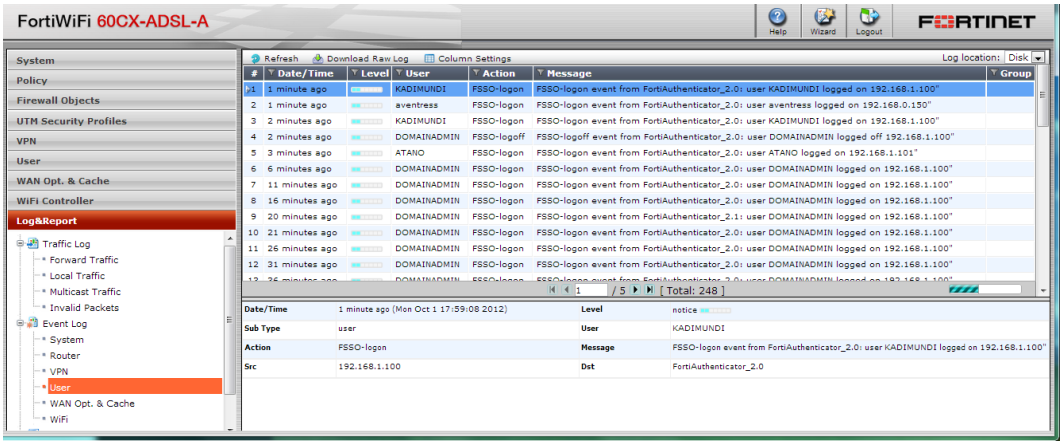



***Double click*** on the entry and the group list should also be visible in the GUI as shown.

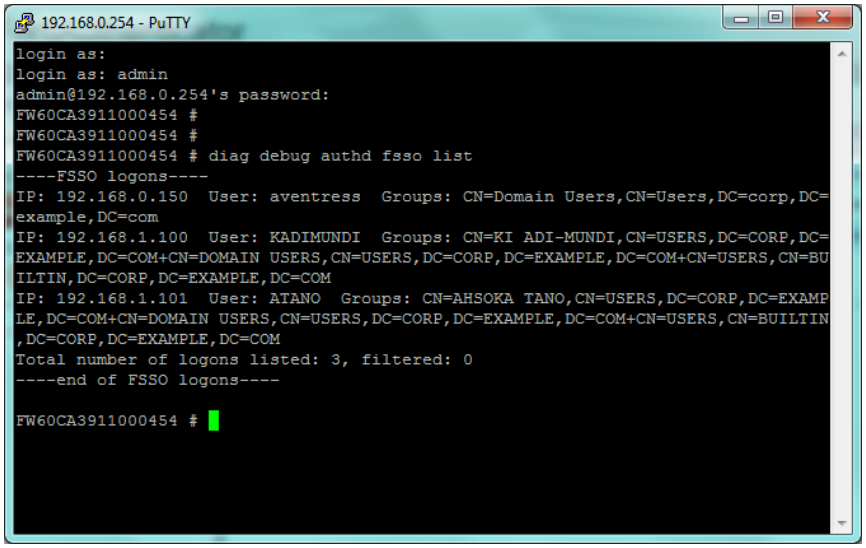



These Groups can be used to differentiate users in Identity Based Policies.

Once the FortiGate device has subscribed to the FortiAuthenticator FSSO Logon Events, any subsequent authentication events should be visible to the FortiGate e.g. in Log & Report → Event Log → User (note that the FortiGate GUI does not appear to display the group detail).



and on the CLI via the command diag debug auth fsso list



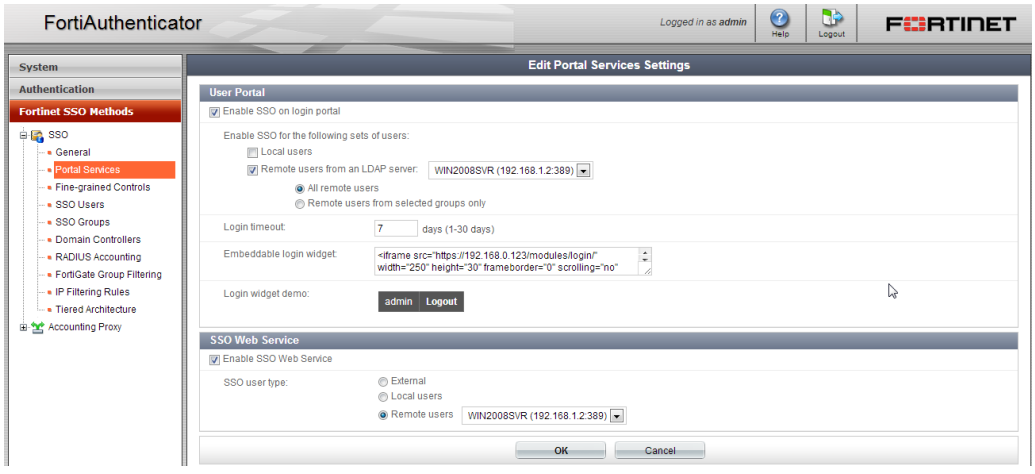

See the FortiGate FSSO Guide for details of how to apply these username/group pairings to Identity Based Policies http://docs.fortinet.com/auth.html .

## Testing

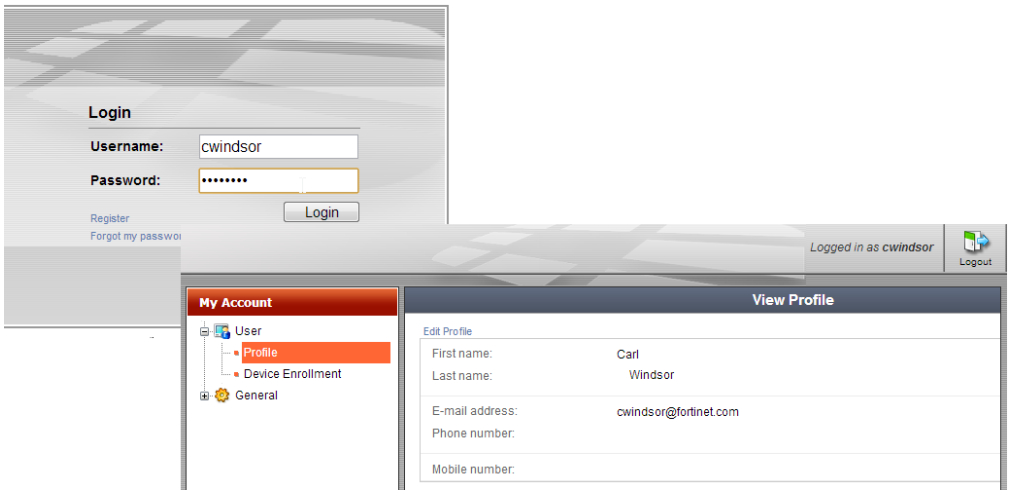
To verify that the communication is set up correctly, a simple authentication event can be sent by authenticating a remote user to the portal. On the FortiAuthenticator, enable portal based authentication:

Browser to *Fortinet SSO Methods → SSO → Portal Services* and *Enable SSO Login Portal*.

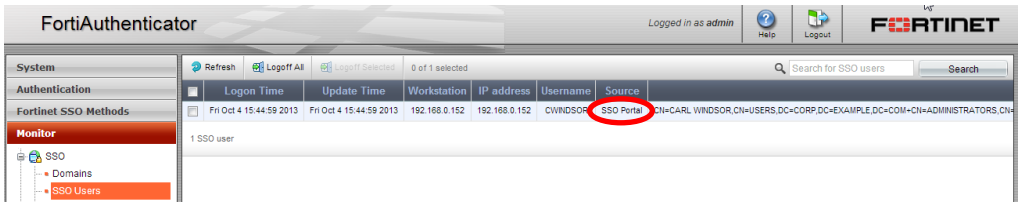
Under *Enable SSO for the following set of users*, select ***Remote users*** *from an LDAP Server* and select the previously configured LDAP directory.




Using a different PC to that being used for administration (or using a different browser or the browsers incognito mode), log in to the FortiAuthenticator portal as the remote user.




This login event should appear under *Monitor → SSO → SSO Users*




….and also on the FortiGate FSSO table as displayed using diag debug authd fsso list.

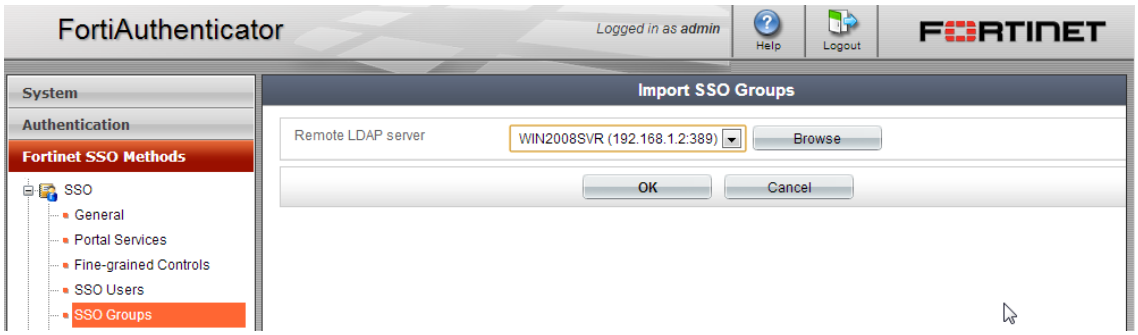
```
FW60CA3911000454 # diag debug authd fsso list
----FSSO logons----
IP: 192.168.0.152  User: CWINDSOR  Groups: CN=CARL
WINDSOR,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM+CN=ADMINISTRATORS,CN=BUILTIN,DC=CORP,D
C=EXAMPLE,DC=COM+CN=DENIED RODC PASSWORD REPLICATION
GROUP,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM+CN=DOMAIN
ADMINS,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM+CN=STAFF,CN=USERS,DC=CORP,DC=EXAMPLE,DC
=COM+CN=FW_ADMIN,DC=CORP,DC=EXAMPLE,DC=COM+CN=SSL_USERS,DC=CORP,DC=EXAMPLE,DC=COM
+CN=DOMAIN USERS,CN=USERS,DC=CORP,DC=EXAMPLE,DC=COM  Workstation: 192.168.0.152
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----

FW60CA3911000454 #
```

## Configure FortiAuthenticator Group Filtering (optional)

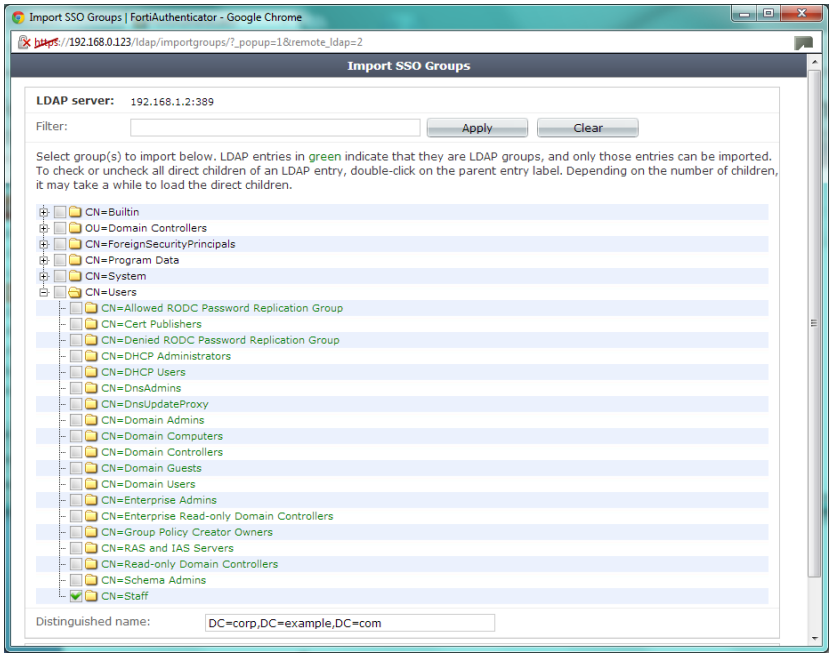
Optionally, the administrator can choose to only send user authentications from specific group members to a FortiGate. This can be used to separate users across physical devices for the purpose of scalability. To configure this feature:

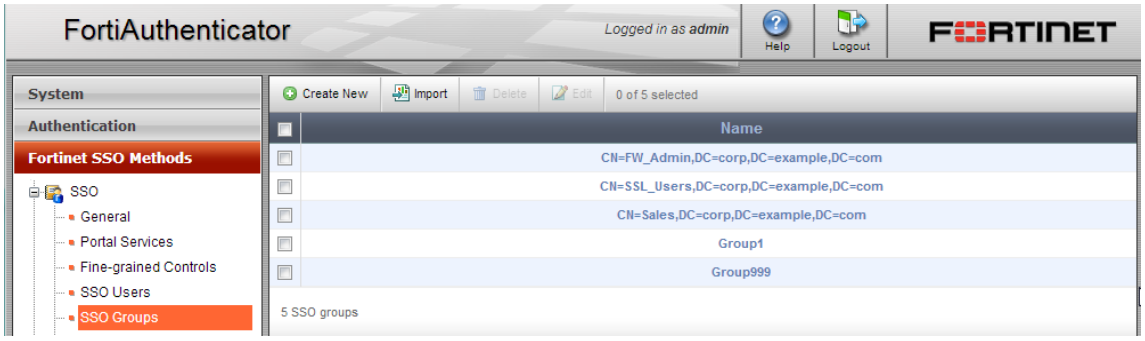
Browse *to Fortinet SSO Methods → SSO → SSO Groups* and select ***Import***

Select the remote LDAP server and select ***Import Groups***



Select the groups which you wish to trigger an FSSO Login event and click ***OK***.

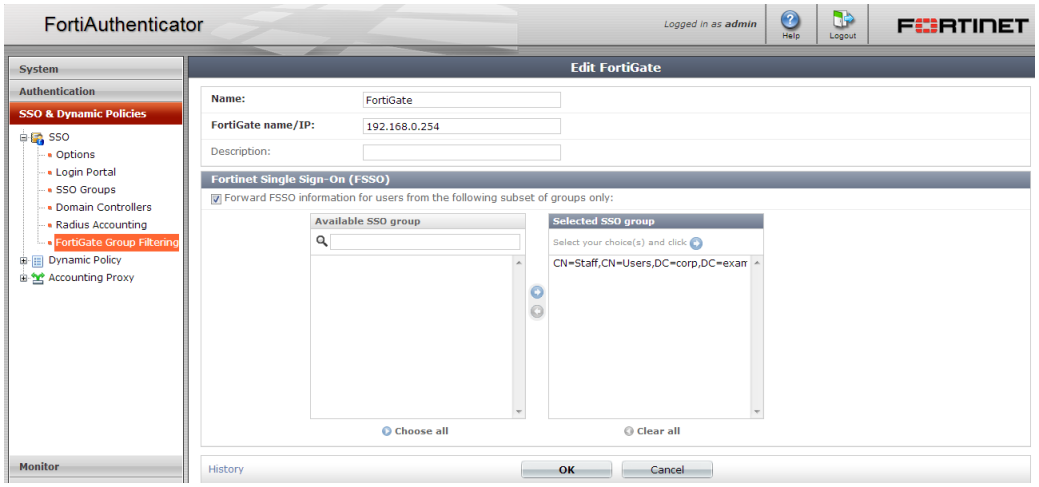



To apply the group specific login events to dedicated FortiGate devices, it is possible to apply specific filtering policies to a device.

Browse *to SSO → FortiGate Group Filtering* and edit the profile of the required device

Enable the checkbox "*Forward FSSO information for users from the following subset of groups*"



## Configuring System Time

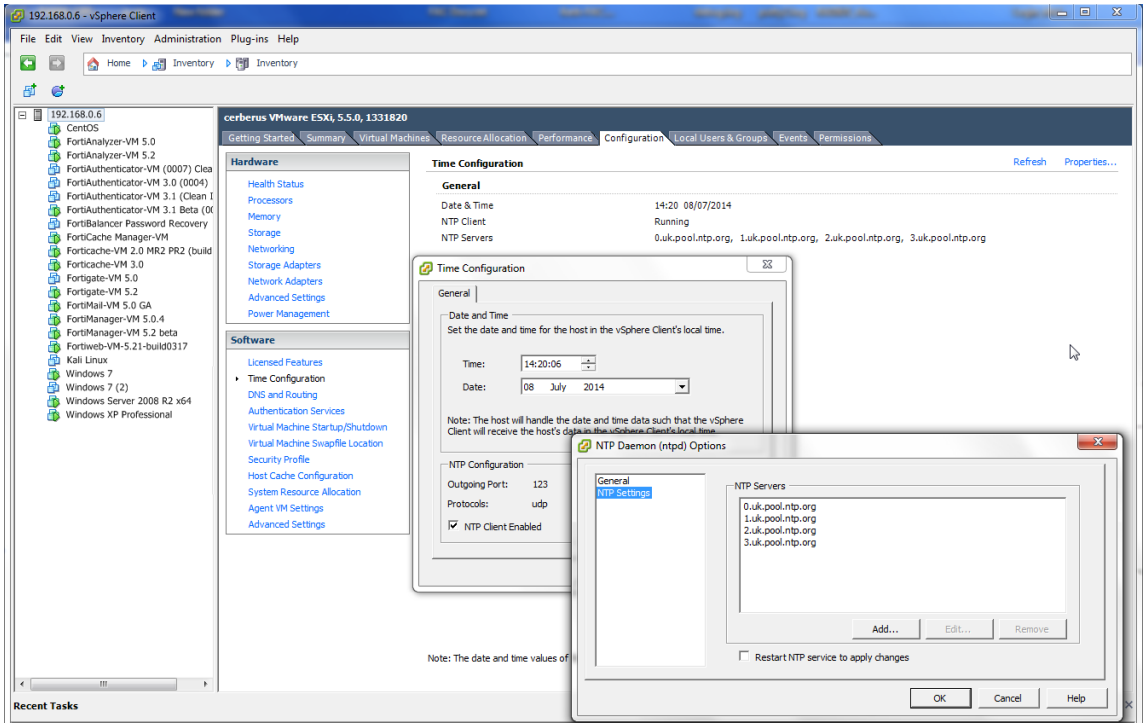
Accurate time is of critical importance to FortiAuthenticator for two factor authentication methods hich can be derived from the time (TOTP). Similarly, accurate system time is critical to some SSO mthods. For example, in the Kerberos protocol, a short lifetime for tickets is used to prevent attackers from performing successful brute force attacks or replay attacks. Any skew in time between systems can cause tickets to be rejected and the authentication process to fail. It is therefore important for all systems within the chain of trust to have accurate time.

Where possible, all systems should use NTP time to synchronise their clocks with the exception however of when running in a virtual environment.

### Configuring host time synchronization (VMWare ESXi)

To configure NTP for the host ESXi VM Server

- Select the server and ***click*** *Configuration*.
- Select *Software >Time Configuration,* ***enable*** the *NTP client and* ***click*** *Advanced*
- Select *NTP Settings* and enter the details of the preferred NTP server.

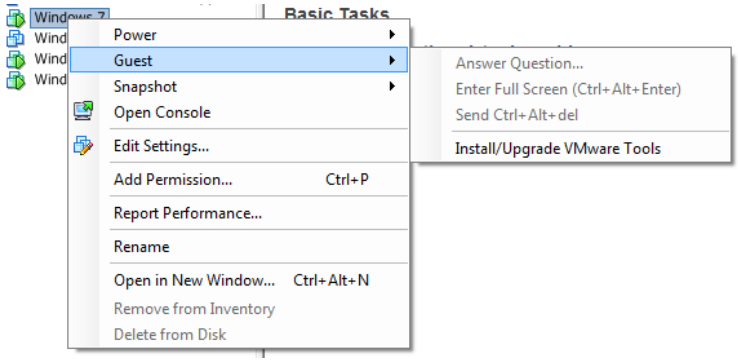



### Configuring VM time synchronization (VMWare ESXi)

In virtual environments, the VM host controls the system time directly via emulation of the Real Time Clock which is kept in sync via the VM Ware tools. Enabling an additional layer of time control via NTP can trigger oscillation between values which is to be avoided.

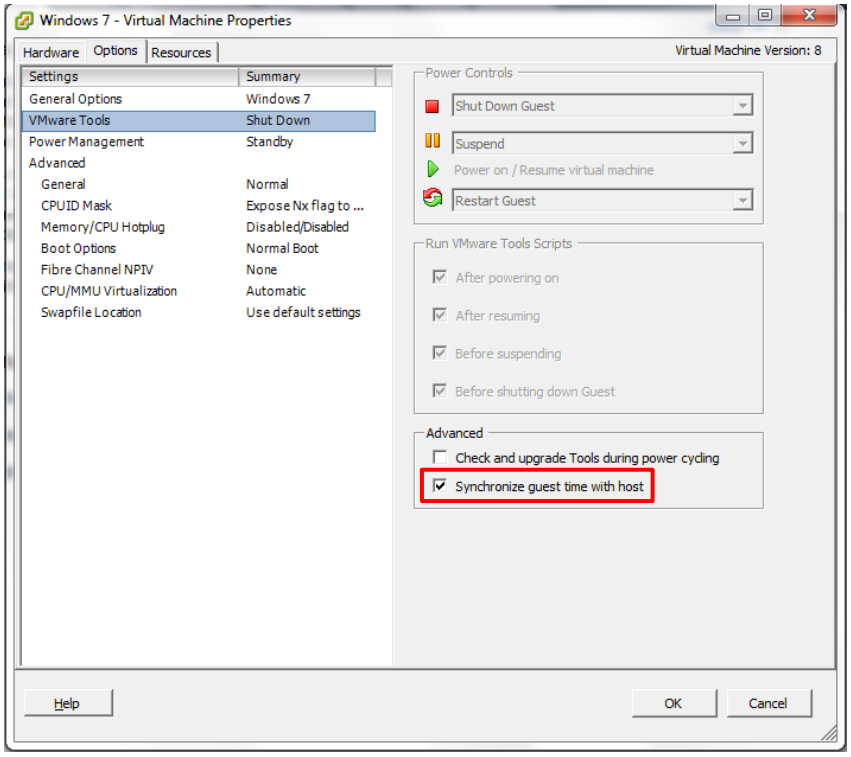
To enable time synchronisation on vritual systems such as Windows Domain controllers or Client OS such as Windows 7, 8 in a virtual environment first, install the VMWare Tools:

- ***Right mouse click*** on *Guest OS* and ***select*** *Guest > Install/Upgrade VMWare Tools*
- Follow the instructions to complete the installation




Once installed, enable the guest time synchronisation:

- ***Right mouse click*** on the Guest VM, and ***select*** *Edit Settings*.
- ***Select*** *Options* and *VMWare Tools*
- Under *Advanced*, ***select*** *Synchronize guest time with host*




Repeat this process for all supported Guest OS includign the Domain Controller and any Guest OS.

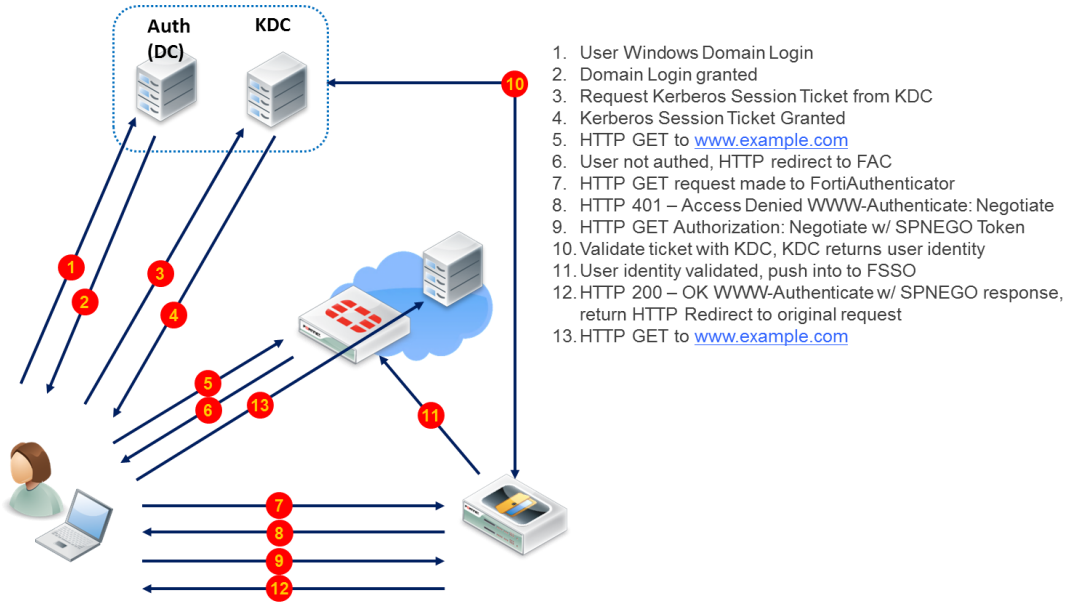
# Kerberos Authentication

**Note:** FortiAuthenticator supports the Microsoft implementation of Kerberos only.

**Note:** Before proceeding, ensure all systems have synchronized time as described in Configuring System Time. Without this, Kerberos authentications will fail.

Kerberos is a system of authentication uses encryption technology and a trusted third party, an arbitrator, to perform secure authentication on an open network. Specifically, Kerberos uses cryptographic tickets in order to avoid transmitting plain text passwords over the wire.

Kerberos is a complicated protocol, but the process has been summarized in the diagram below.

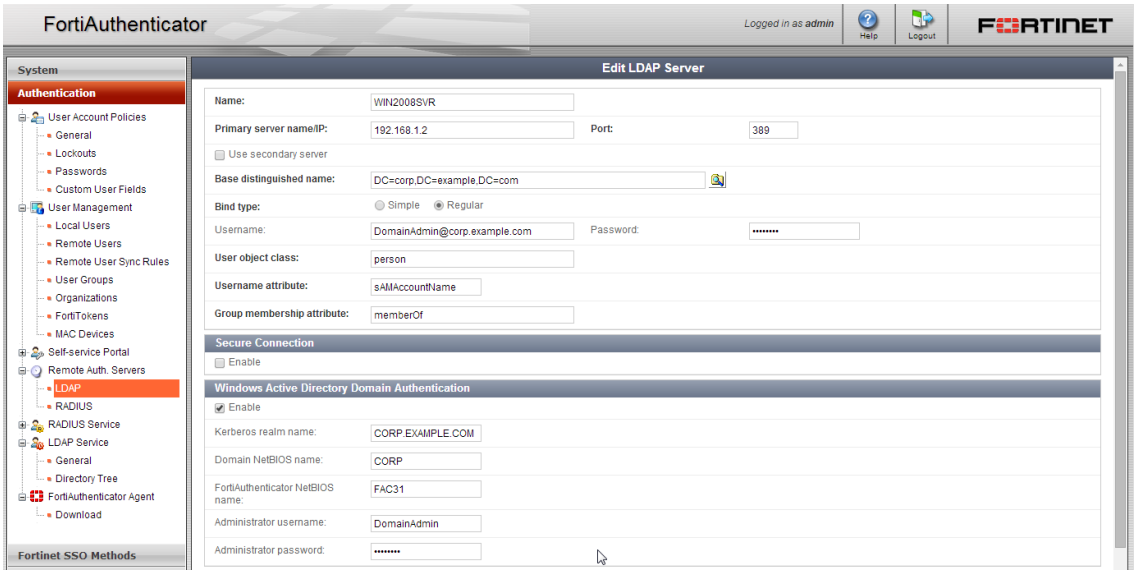



## Configure FortiAuthenticator on the Windows domain

The required LDAP configuration is documented in the section FortiAuthenticator FSSO Authentication, however additional steps are required for successful Kerberos authentication.

Enable Windows Active Directory Domain Authentication and configure appropriately e.g.

```
Kerberos realm name:                CORP.EXAMPLE.COM
Domain NetBIOS name:                CORP
FortiAuthenticator NetBIOS name:    FAC31
Administrator username:             DomainAdmin
Administrator password:             <password>
```

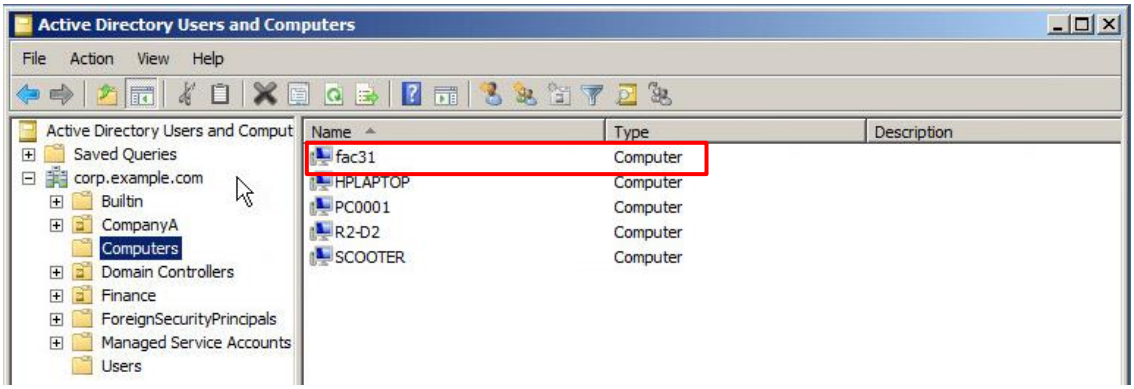



FortiAuthenticator NetBIOS name should match the system hostname

The Administrator username should have permission to join computers to the domain (e.g. Doman Admin)

- Select ***OK***.

Once complete verify that the FortiAuthenticator is registered as a machine on the domain

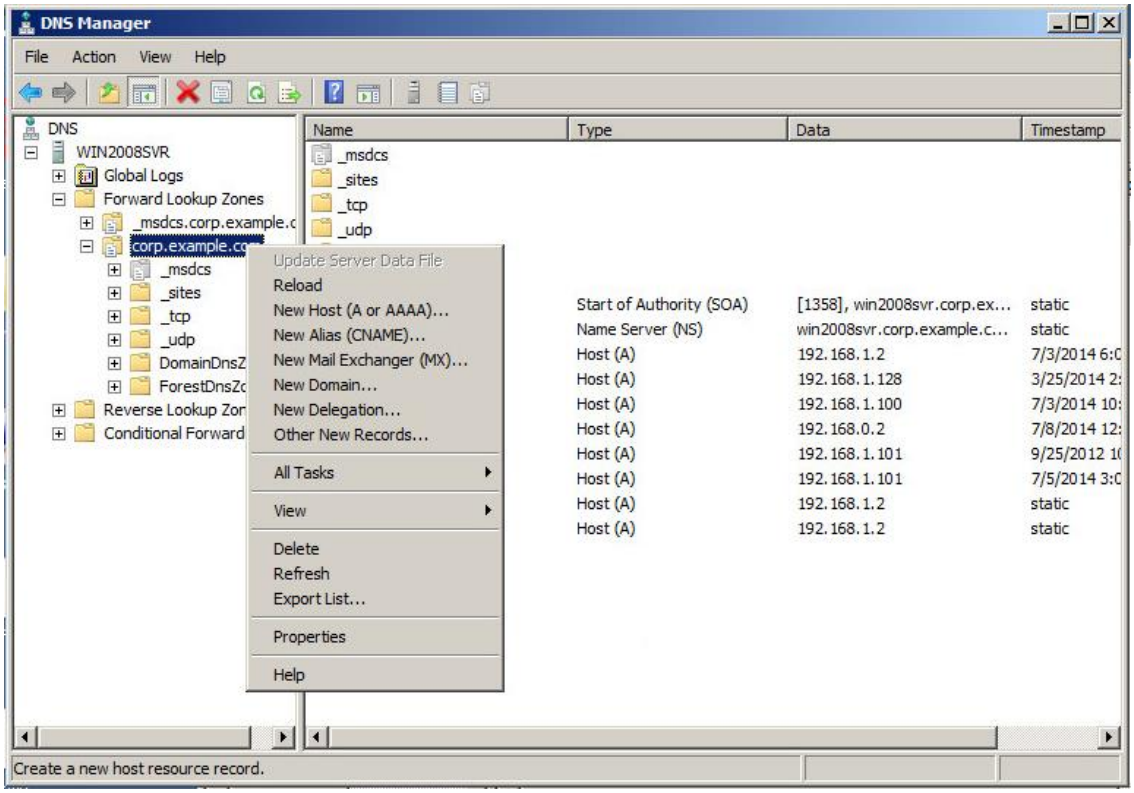



## Configure FortiAuthenticator in DNS on the Windows domain

All systems involved require to be able to resolve the FQDN of the FortiAuthenticator from DNS. To achieve this all systems need to use the domain configured DNS and an A record needs to be configured.

To create the DNS record on the Windows Domain:

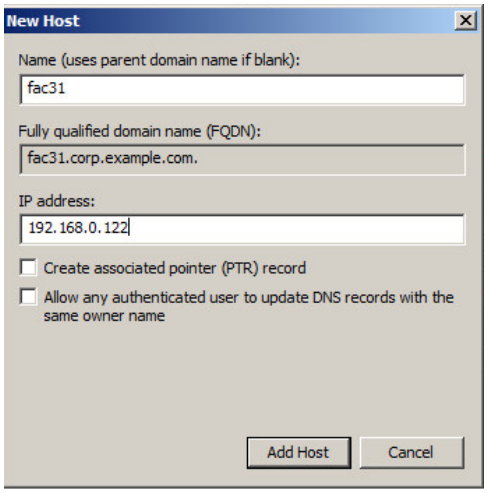
- On the Windows Domain Controller, ***open*** the *DNS Manager* and ***right mouse click*** the Domain in which the FortiAuthenticator resides and ***select*** *New Host (A or AAAA).*




- In the New Host dialog, enter the Name and IP address of the FortiAuthenticator e.g.

  `Name:` `fac31`

  `IP address:` `192.168.0.122`




Verify that all systems can resolve the DNS name, including the FortiAuthenticator and FortiGate

```
> nslookup fac31.corp.example.com
Server:    192.168.1.2
Address 1: 192.168.1.2

Name:      fac31.corp.example.com
Address 1: 192.168.0.122
```

## Create the Keytab file

The Keytab file tells FortiAuthenticator how to interact with Kerberos e.g where and with which credentials. To generate this file, you can use the Windows ktpass utility. The following batch file to simplify creation of the keytab file.

**Gen_Keytab.bat**

```
set OUTFILE=c:\fac31.keytab

set USERNAME=KrbSvcUser@corp.example.com

set PRINC=HTTP/fac31.corp.example.com@CORP.EXAMPLE.COM

set CRYPTO=all

set PASSWD=pa$$w0rd

set PTYPE=KRB5_NT_PRINCIPAL

ktpass -out %OUTFILE% -pass %PASSWD% -mapuser %USERNAME% -princ
%PRINC% -crypto %CRYPTO% -ptype %PTYPE%
```

Pay specific attention to capitalization in the file, ensuring it is replicated as shown. Ensure that the batch file is run with Administrator privileges. To do this, and see errors returned when running, ***click*** *Start Menu* and ***right mouse click*** on the *Command Prompt*, ***selecting*** *Run as Administrator*. Once run, the batch file shown should output a file named c:\fac31.keytab. Copy this field to the desktop, it will be used in a subsequent step.

The username specified within the Keytab (KrbSvcUser@corp.example.com) needs only to be a normal Domain User, not Domain Admin.

It is possible if the KeyTab has been generated multiple times or for multiple systems, that several servicePrincipleName entries exist. To check for this, the following command can be run:

```
ldifde -f check_SPN.txt -t 3268 -d "" -l servicePrincipalName -r
"(servicePrincipalName=HTTP*)" -p subtree
```

If multiple entries exists as shown, the spurious and additiona SPN entries should be removed

**check_SPN.txt**

```
dn: CN= KrbSvcUser,CN=Users,DC=corp,DC=example,DC=com

changetype: add

servicePrincipalName: HTTP/fac31.corp.example.com

servicePrincipalName: HTTP/fac30.corp.example.com
```

Only a single SPN entry should exist and it should be for the FAC that the Keytab file will be loaded onto, If multiple keytabs are required, use multiple user accounts to create them. To remove spurious SPN entries:

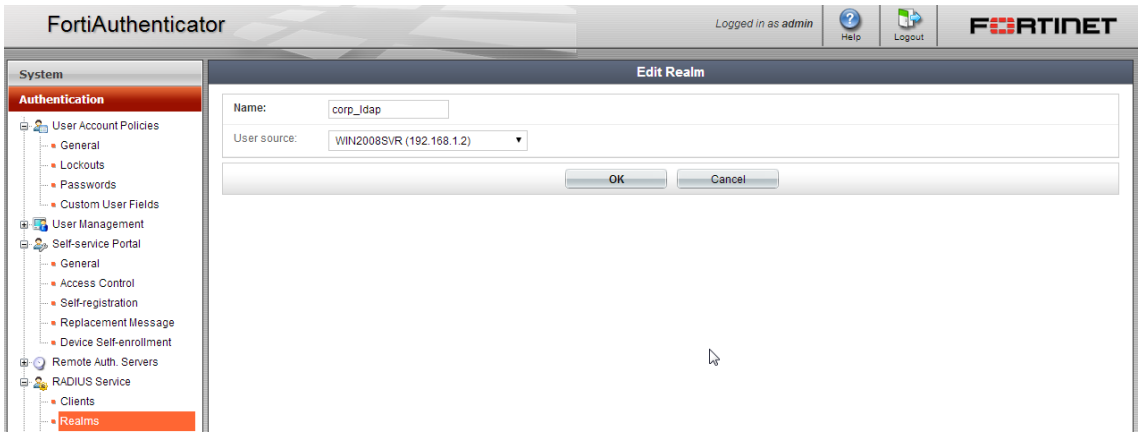
```
setspn -D HTTP/ HTTP/fac30.corp.example.com KrbSvcUser
```

## Enable the Kerberos Authentication Portal

The next 2 steps involve configuration within the Authentication section which is not necessarily intuitive.

## Create a Realm

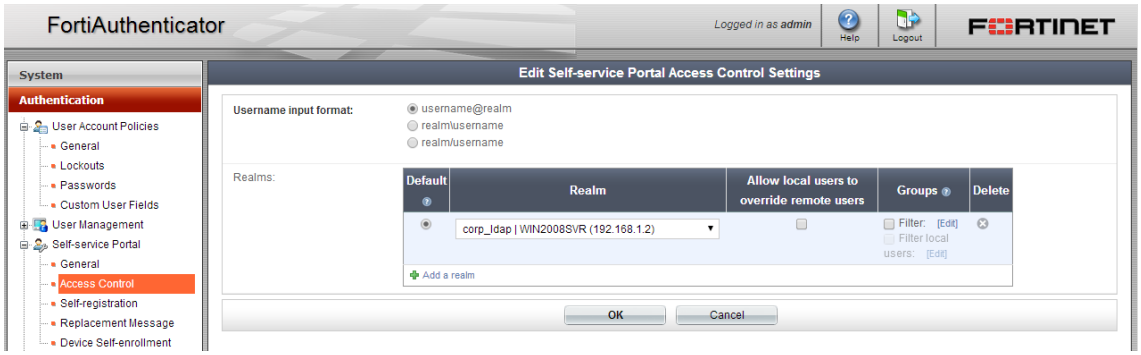
- Browse to Authentication > RADIUS Service > Realms and select New.
- Select the relevant LDAP directory and ***enter*** a realm name.
- ***Click*** *OK*




## Configure the User Portal Access Control

It is not possible to directly add a new realm to the User portal (*Fortinet SSO Methods > Portal Services*). To achieve this, the realm must be added under *Authentication > Self-Service Portal > Access Control.*

- ***Browse*** to this location then and click *Add a Realm and select the realm created in the previous step.*
- Depending on your requirements, the *Local user* realm can be removed.



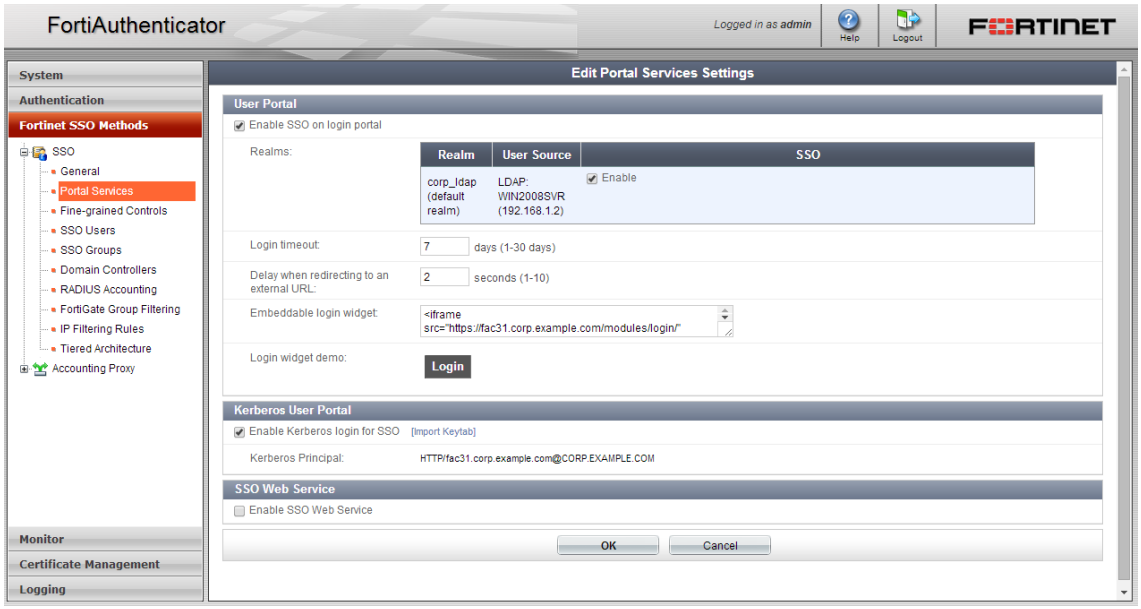

Once complete, it is possible to procede and configure the User Portal

## Configure the User Portal

On the FortiAuthenticator browse to *Fortinet SSO Methods > SSO > Portal Services*

- ***Select*** *Enable SSO on Logon Portal. Notice the realms specified in the previous Access Control* step are now displayed. The Kerberos portal inherits these permissions from the User Login portal.
- ***Click*** *Import Keytab* under *Kerberos User Portal*.

Once the Kerberos Principle field is correctly configured, Select Enable Kerberos for SSO to enable the portal.

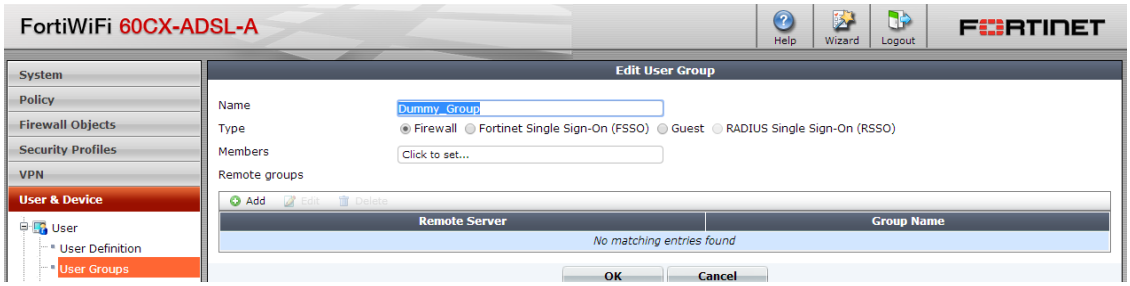



## FortiGate Configuration

To enable Kerberos Single Sign-On FortiGate is configured to authenticate users into an Identity Based Policy in the first instance, and if this fails, fall back to a policy which redirects the user to the FortiAuthenticator to authenticate the user via Kerberos. To achieve this the following steps must be taken.

### Create a dummy authentication group

The dummy authentication group is used as the fallback rule only to redirect unauthenticated users to the FortiAuthenticator. As such, no authentication is required to be configured.




**CLI Configuration:**

```
config user group
    edit "Dummy_Group"
    next
end
```

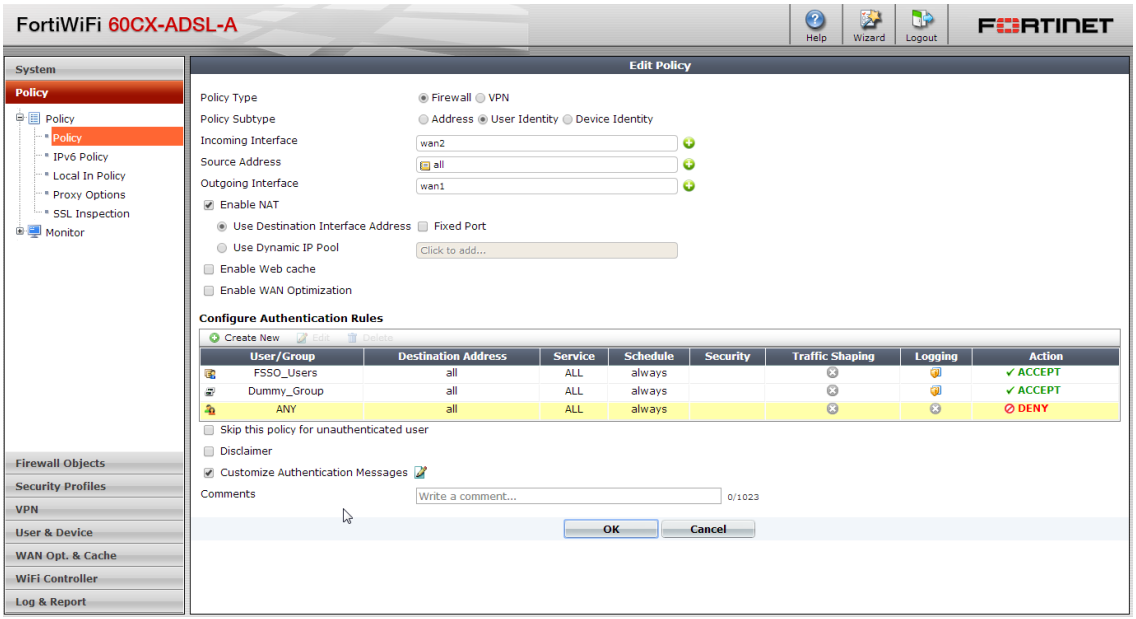
### Firewall Policy Flow

The firewall policies must be configured to allow any essential internal traffic prior to traffic requiring authentication. This may include exclusion policies to allow as a minimum:

- DNS
- DHCP
- All traffic to FortiAuthenticator

Additional policies may be required to enable access to local domain controllers, internal fileshares and other resources

Once this traffic is allowed, the firewall policy requiring authentication will be reached. A user Identity Based Policy should be configured with an FSSO rule to match existing known users with a fall back rule pointing at the Dummy User Group which will be used to redirect unknown users to the FortiAuthenticator for Kerberos Authentication.




Instead of providing manual Firewall authentication in the Dummy_Group rule, the Login Portal Page is rewritten as a redirect to the URL of the FortiAuthenticator. It is essential at this stage that the URL of the FortiAuthenticator is used, not the IP address, and it matches that of the URL specified in the Kerberos Principle Name.

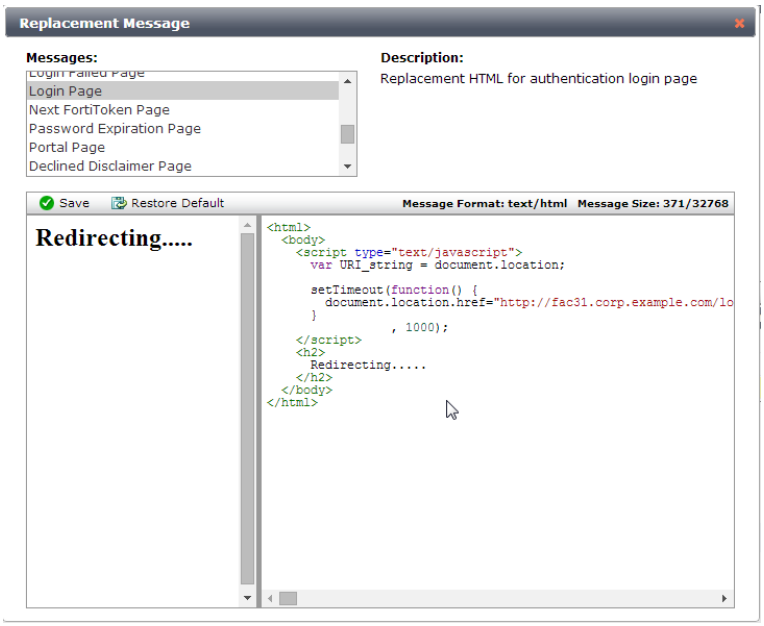
## Enabling the Redirect Portal

Enable customise Authentication Messages and edit the Login Page.


Replace the existing HTML with the following:

```
<html>
  <body>
    <script type="text/javascript">
      var URI_string = document.location;

      setTimeout(function() {
```

```
document.location.href=http://fac31.corp.example.com/login/kerb-
auth?user_continue_url= %%PROTURI%%;
      }
                  , 1000);
    </script>
    <h2>
      Redirecting.....
    </h2>
  </body>
</html>
```




## Internet Explorer Configuration

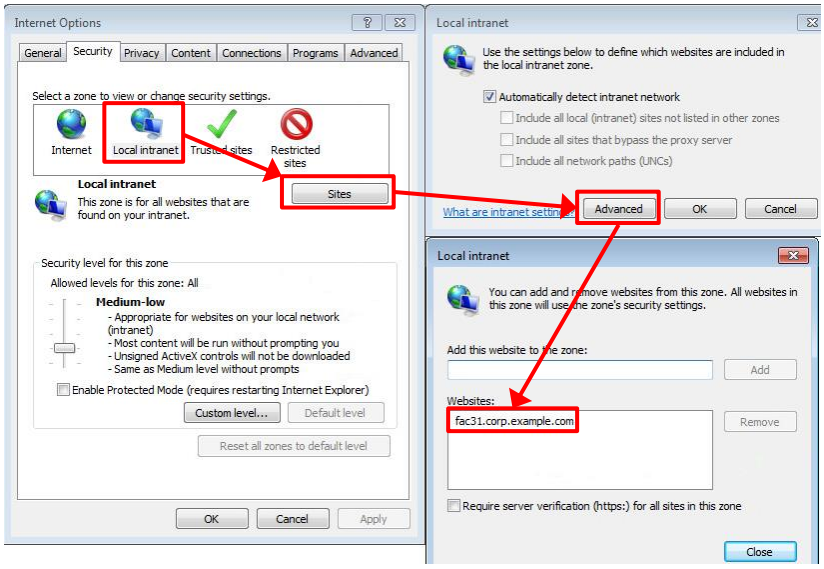
This setup relies on a few important key factors:

- Kerberos is supported by the browser and enabled
- Time is correctly synchronized on all devices
- FortiAuthenticator is added to the local security groups (see below)

### Adding FortiAuthenticator to the Local Intranet sites

**Note:** If this step is omitted, users will be prompted for authentication credentials, which will fail. This can be done manually or pushed out via Group Policy.

- Open Internet Explorer
- Click the Advanced Options and go to the Security Tab.
- Select the Local Intranet option
- Click the “Sites” option and ***select*** *Advanced.*




- Add the FortiAuthenticator URLs to the local Intranet zone. For example: `fac31.corp.example.com` (note no need for HTTP/S)
- Click “Close.”

## User Experience

When users login and open Internet Explorer, the user should see:

- On initial login and first web page opened, a page that says redirecting..
- After a short period of time, the user’s page should display.
- Additional pages should not display redirecting.

**Successful Logon**


## Troubleshooting

**Error :Kerberos authentication is not available.**

Verify that the Kerberos portal is enabled in *Enable Kerberos Login for SSO.*

**Error: 404 Not Found error on redirect**

Verify the URL being redirected to is correct. If the original URL requested was http://www.google.com the URL redirected to on the FortiAuthenticator should be

```
http://<FAC_URL>/login/kerb-
auth?user_continue_url=http%3A%2F%2Fwww.google.com%2F
```

Note that it is critical that the URL is used not the IP address and that this matches the FQDN specified in the Keytab file.

**Error :Kerberos authentication is failing.**

Verify that:

- Time is synchronised between all systems

- The Keytab file has been configured correctly (note case used in the example file)
- Access controls have been accurately configured

**Error: Repeated authentication “Redirecting”**

Suggests Kerberos authentication is working and FortiAuthenticator is redirecting, however, the authentication event is not reaching the FortiGate. Verify:

- The FGT is not receiving FSSO events correctly
- That the user is not being NATed and that the IP identified by the FAC matches that identified by the FGT.

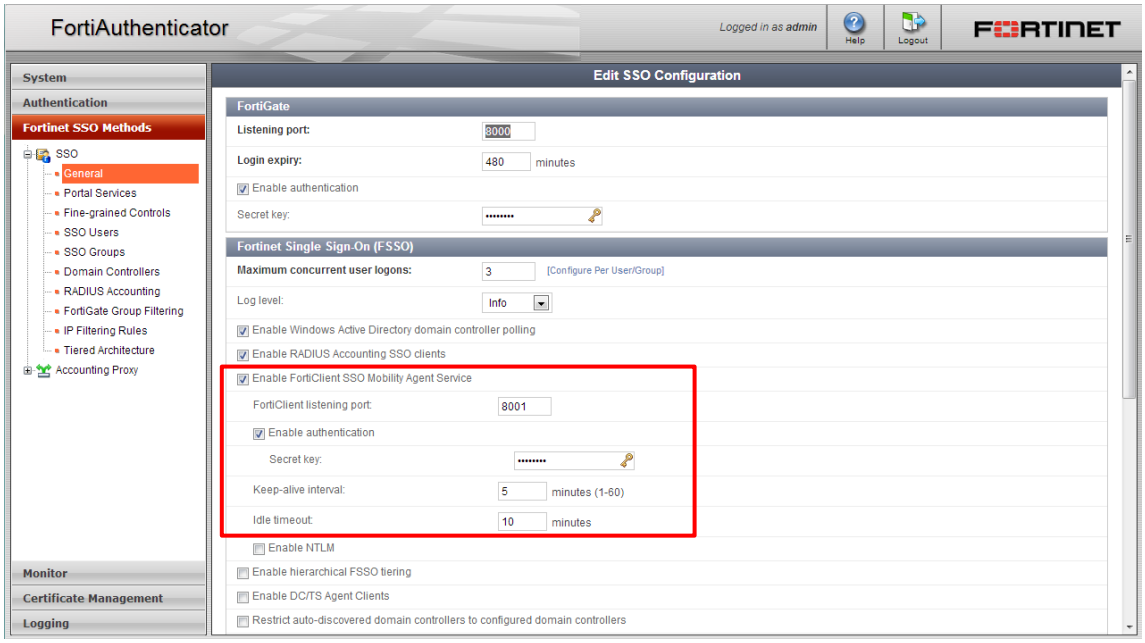
# FortiClient Single Sign-On Mobility Agent

FortiClient Single Sign-On Mobility Agent is a feature of FortiClient v.5.0. The FortiClient software identifes the logged in domain user and IP address and communicates this information to the FortiAuthenticator. The FortiClient SSO Mobility Agent has several benefits over other FSSO detection methods:

- FortiClient sends regular HELLO packets. If FortiAuthenticator detects X missing HELLO packets, the user is deauthenticated.
- If the device IP stack changes e.g. roaming on the wireless network, the update is sent to the FortiAuthenticator
- If the user logs out, the FortiClient notifies FortiAuthenticator on shutdown and de-authenticates the user.

To configure service FortiClient Single Sign-On Mobility Agent service:

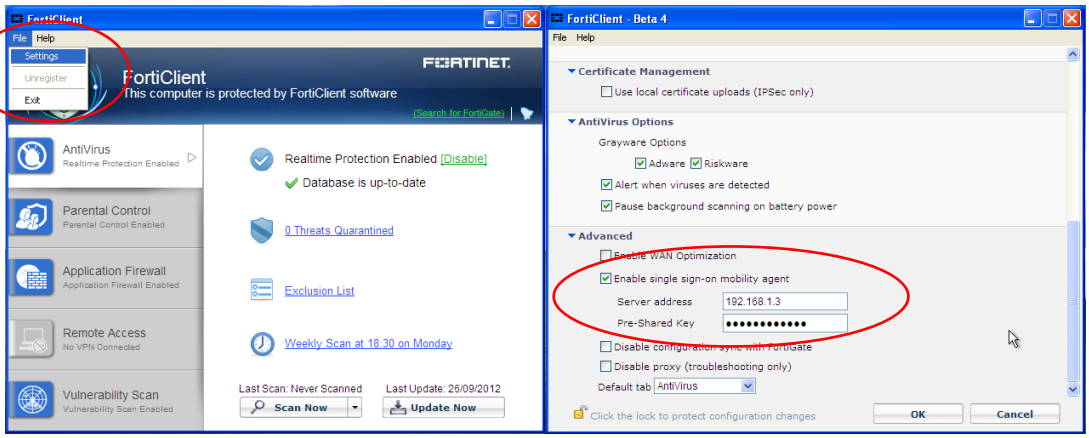
- Browse to *Fortinet SSO Methods → Options* and under the section *Fortinet Single Sign-On (FSSO)*, select ***Enable FortiClient Service***.
- Set the port and secret key to an appropriate value (***default port for FortiClient is 8001***)




To configure service FortiClient Single Sign-On Mobility Agent on the endpoint:

- Obtain the FortiClient 5.0 software from the Fortinet Support Web Site http://support.fortinet.com (may require logon).

- Install the FortiClient software on the required PC as per the software installation instructions
- As a user with system administration credentials, browse to *File → Settings* in the FortiClient GUI. Note that the *Settings* configuration will not be available to normal, low privilege users
- Scroll to the bottom of the settings page and check the box to ***enable single sign on mobility agent***
- Enter the IP address of the FortiAuthenticator in the *Server Address* field. Note that the default port in FortiClient is set to 8005. If an IP address is specified without a port, the default will be used. To specify an alternate port, use the format <FAC_IP>:<PORT> e.g. 192.168.0.123:8001.
- Enter the pre-shared key as defined on the FortiAuthenticator.




To validate successful communication, log out of the end point and back in then check the FortiAuthenticator in Monitor → SSO Users for events with the source FortiClient.


## Repackaging the Mobility Agent Component

If installation of the full FortiClient is not necessary or required, it is possible to repackage FortiClient to only install the Mobility Agent component. To do this, acquire the repackaging components in the FortiClientTools file from https://support.fortinet.com and a license for the repackager.

**Note:** There is only a 32bit version of the repackaging utility. You don't need a 64bit version of the repackager to create a 64bit installer.

**Note:** Before proceeding, a license is required to use the features of the FortiClient Configurator tool. Contact Fortinet support for details.

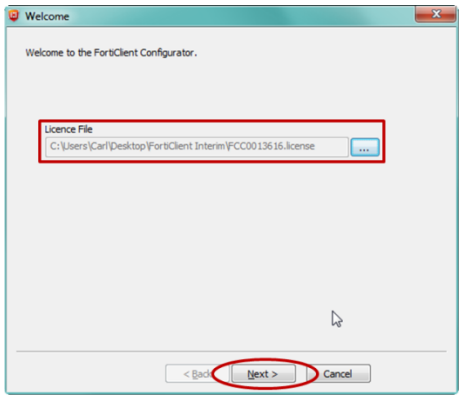
- Unpack the Zip file and locate the FortiClient Configurator utility folder.
- Create a configuration file to tell the FortiClient Configurator utility how to configure the repackaged client.

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
    <fssoma>
        <enabled>1</enabled>
        <serveraddress>192.168.1.123:8001</serveraddress>
        <presharedkey>fortinet1234</presharedkey>
    </fssoma>
</forticlient_configuration>
```

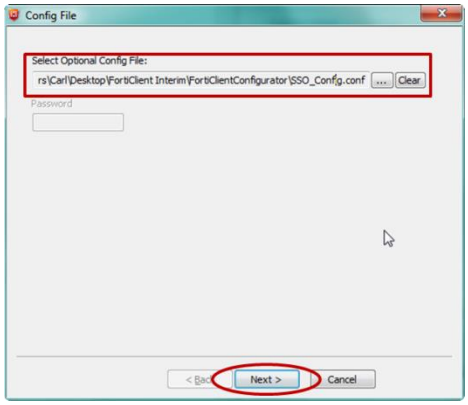
Where:

| | | |
|---|---|---|
| <serveraddress> | = | The IP or FQDN of the FortiAuthenticator and the communication port (default port is 8001) |
| <presharedkey> | = | The authentication key used to validate communication with the the FortiAuthenticator |

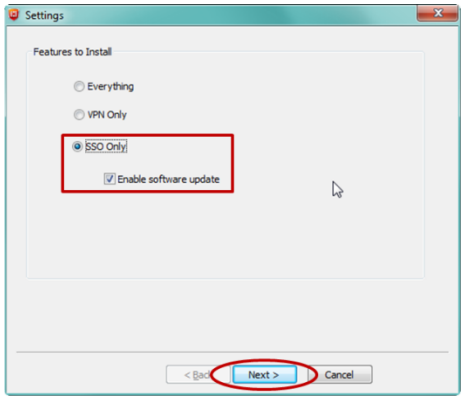
- In the FortiClientConfigurator folder run FortiClientConfigurator.exe (Admin privileges may be required) and follow the on screen instructions.
- Select the location of your license file and click Next



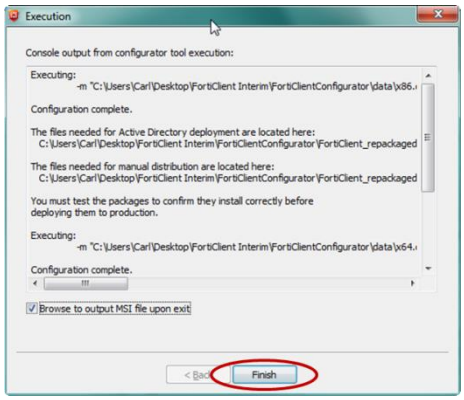

- Select the configuration file created in the previous step




- Chose SSO Only. This will remove all other components from the installation. ***Click*** *Next.*



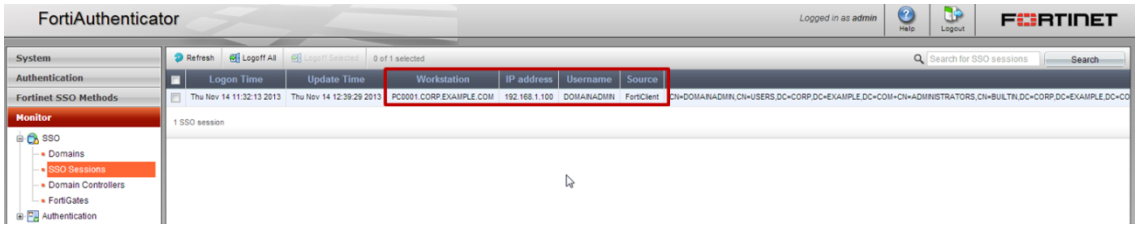

- The Configurator will print out the actions and commands that have been executed. ***Click*** *Next*




- The Reconfigured SSO MA Agent MSI files will be output to the folder FortiClient_repackaged in both x64 and x86 versions
- To install, either transfer the files to a system and manually install (elevated privileges required) or use the MSI file to perform a GPO based install.
- Follow the instructions until the install is complete. A reboot should not be required.

## Testing

On the test PC, log out and re login (to trigger the client). On the FortiAuthenticator browse to the Monitor > SSO > SSO Sessions and look for the new FortiClient Sourced Login Event



# Portal Authentication

The FortiAuthenticator Single Sign-On Portal consists of 2 main components,

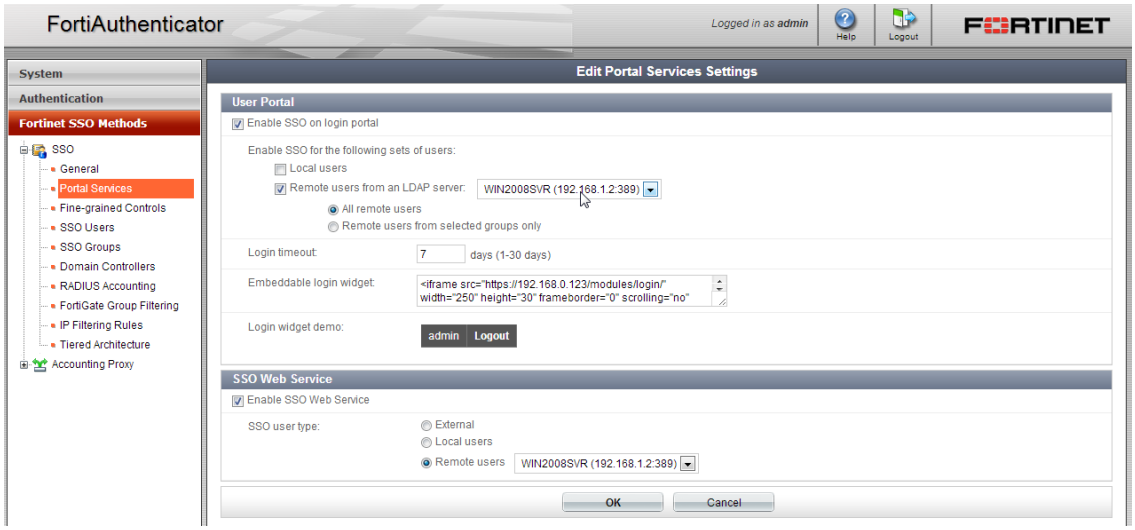
**Login Portal** Manual authentication portal for use in situations where dynamic, transparent authentication has failed or has not been possible.

**Login Widgets** Set of web widgets which can be embedded into an organizations intranet home page to assist in the authentication process.

## Configure the login portal

To enable the Fortinet Single Sign-On Portal:

- Browse to *Fortinet SSO Methods → Login Portal* and *select* ***Enable SSO Portal***
- Select the locations with which to authenticate the users. In the example below, the portal will authenticate users against the local user database and the remote LDAP/AD WIN2008SVR.




## Redirecting user to the FortiAuthenticator portal

To authenticate users via the Fortiauthenticator portal, traffic must be redirected to it from the FortiGate. The workflow for this is:

- User logs into their PC
- User browses to a FortiGate protected resource e.g. Internet
- If FGT attempts to identify the user via FSSO (this may be via SSOMA, Polling etc or a previous Portal authentication)
    - If authenticated, grant appropriate access
    - If not authenticated, redirect to the FAC to authenticate
- FAC authenticates user and redirects the user back to the originally requested URL

Once configured, users will be able to log in via the standard FortiAuthenticator GUI and will be confirmed as authenticated.


*Successfully logged in as **aventress**. Please remember to logout when you are finished.*

And the user will be visible in the FortiAuthenticator in *Monitor → SSO Users* with the source type *SSO Portal*.


## Configuring FSSO Widgets

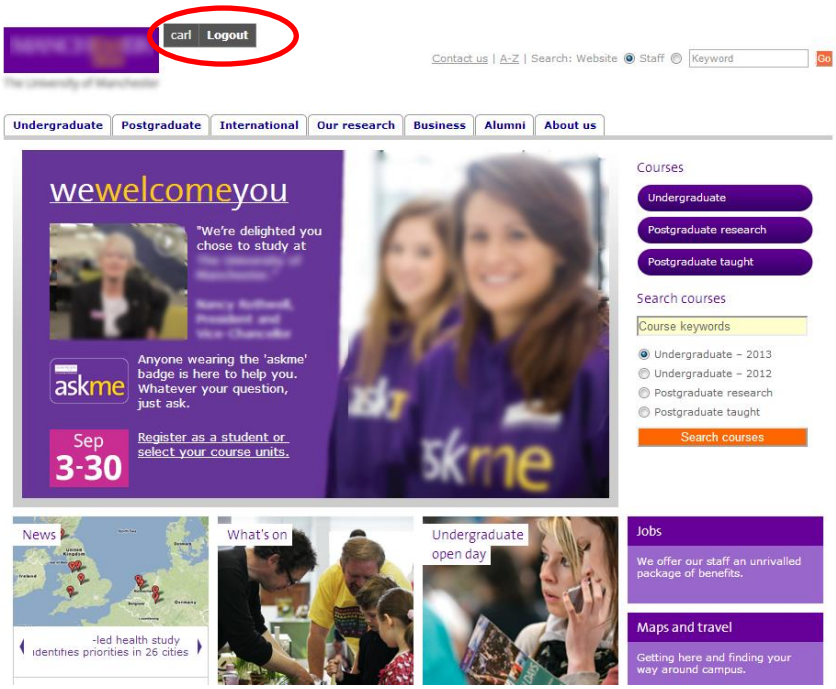
The FortiAuthenticator FSSO Widgets have been designed to reduce the impact of re-authentication. Their purpose is to automate the process of identifying the user with FortiAuthenticator when transparent methods are not possible. The widget sets a cookie in the users browser which is valid for a number of days specified in the Login Portal Configuration. The cookie contains a security string which is associated with the user on the FortiAuthenticator. When an authenticated user logs out and back in again, the widget checks the cookie and will transparently authenticate the user if valid. To take advantage of this feature, the administrator should insert the FortiAuthenticator widget into a convenient web page (such as the organization intranet) and this should be set as the default home page.

To achieve this, the administrator should insert the code displayed at *Fortinet SSO Methods → Login Portal* in the *Embeddable Login Widget* section, into the intranet page in a convenient location.

```
<iframe src="https://192.168.0.123/modules/login/" width="250"
height="30" frameborder="0" scrolling="no"
style="padding:5px;"></iframe>
```

**Caution.** Do not copy the HTML above, always obtain this from the FortiAuthenticator as it will be specific you your installation.

The resulting web page will look similar to the following example and will include the Login Widget iframe.


carl
Logout
Contact us | A-Z | Search: Website Staff Keyword Go
Undergraduate
Postgraduate
International
Our research
Business
Alumni
About us
wewelcomeyou
"We're delighted you chose to study at
Anyone wearing the 'askme' badge is here to help you. Whatever your question, just ask.
Sep 3-30
Register as a student or select your course units.
Courses
Undergraduate
Postgraduate research
Postgraduate taught
Search courses
Course keywords
Undergraduate – 2013
Undergraduate – 2012
Postgraduate research
Postgraduate taught
Search courses
News
What's on
Undergraduate open day
Jobs
We offer our staff an unrivalled package of benefits.
Maps and travel
Getting here and finding your way around campus.

# Radius Accounting

## RADIUS Accounting Source

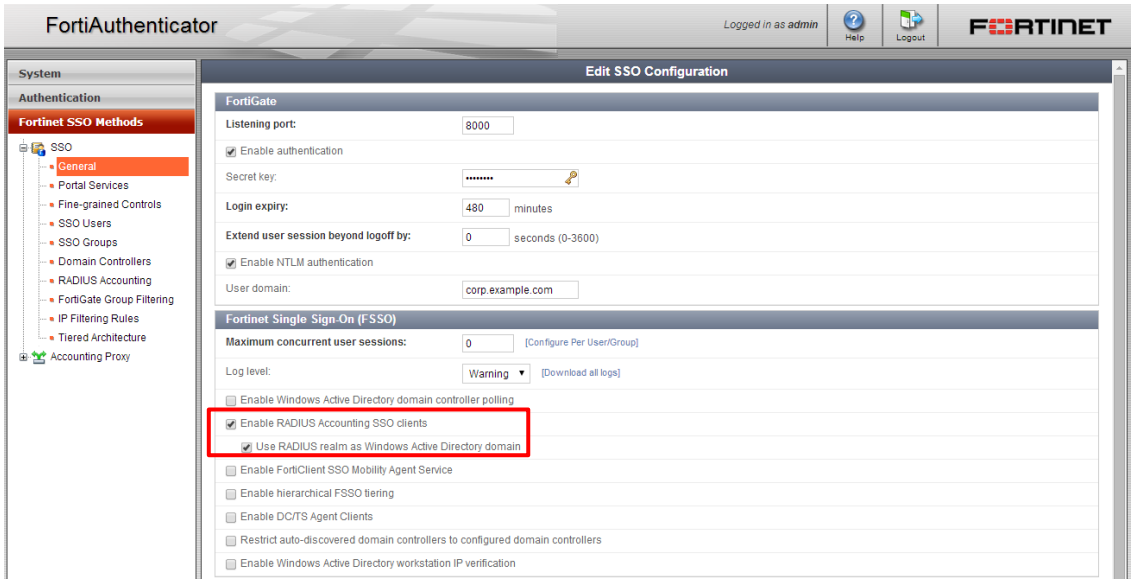
FortiAuthenticator supports the ability to receive RADIUS Accounting packets and use the provided RADIUS Attribute Value Pairs (AVP) as a source of authentication information and then push these events into FSSO.

**Caution:** RADIUS FSSO is a different feature to the RADIUS Accounting Proxy where Accounting packets are received, manipulated and forwarded to multiple destination endpoints. The RADIUS FSSO feature is configured under *Fortinet SSO Methods → SSO* whereas the RADIUS Accounting Proxy is configured under *Fortinet SSO Methods → Accounting Proxy.*

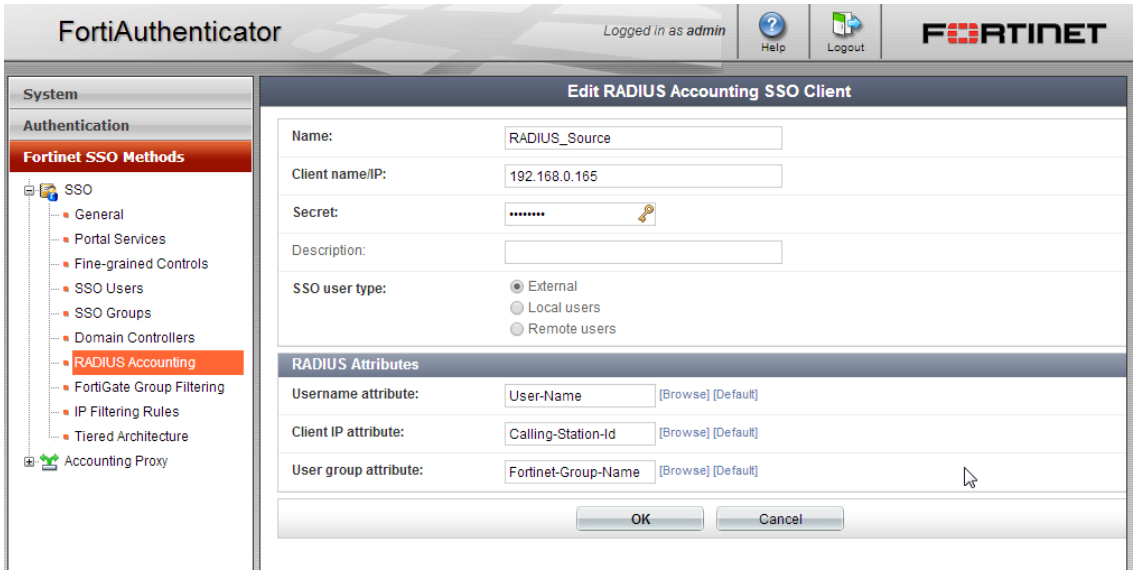
*For more information on the RADIUS Accounting Proxy see the document* ***RADIUS Accounting Proxy Guide*** http://docs.fortinet.com/auth.html

To enable RADIUS as a source of Single Sign-on:

- On the FortiAuthenticator, browse to *Fortinet SSO Methods → SSO → General* and enable the RADIUS Accounting SSO.
- Optionally enable Use RADIUS Realm as Windows Active Directory domain if this is going to be used on a multi-domain environment.




- Browse to *Fortinet SSO Methods → SSO → RADIUS Accounting and select* ***New***
- Create a new entry containing details of the remote RADIUS server which will be supplying the start records. Include a pre-shared key to be used for authenticating the data source




Select the appropriate SSO User Type:

**External:** Users are derived from external source (e.g. RADIUS). Use this method when Username, IP and all relevant group info is defined in the RADIUS packet.

**Local Users:** User and IP info is contained in the RADIUS packet but user is defined locally and additional group info can be sourced from the local group database.

**Remote Users:** User and IP info is contained in the RADIUS packet but user is defined remotely and additional group info can be sourced from the LDAP.

Once this has been configured, it is necessary to configure the RADIUS platform to forward RADIUS accounting packets to the FortiAuthenticator and ensure that the packets contain the required AVPs to trigger the authentication event. The required AVPs are of the format:

```
User-name               = <Username>
Fortinet-Client-IP      = <Client IP>
Fortinet-Group-Name     = <Group Membership>          (Optional)
```

Alternative attributes can be configured under Edit RADIUS Accounting SSO client, and these will automatically be rewritten to the required Fortinet AVPs shown above.

A RADIUS dictionary is available from the Downloads Fortinet Support site https://support.fortinet.com/.

.This may be required by the third party RADIUS vendor to be able to send the required AVPs. All other configuration of the third party RADIUS platform is out of the scope of this document.

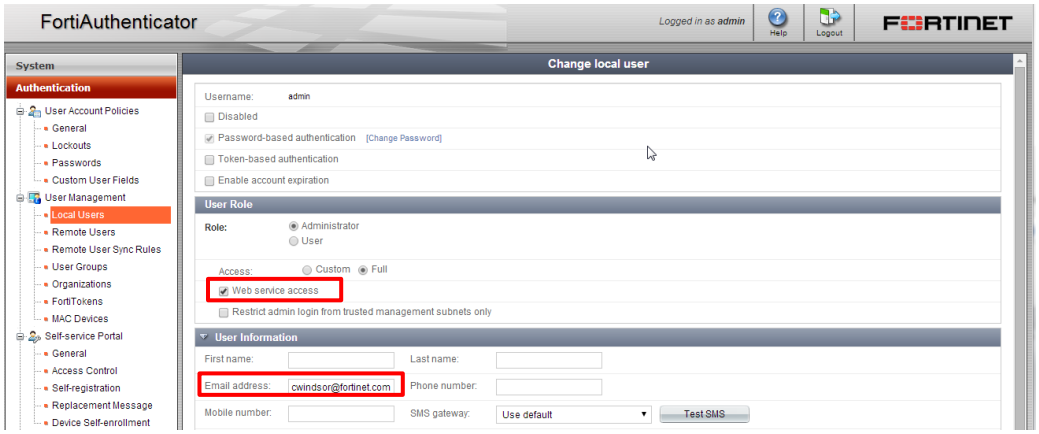
# FortiAuthenticator API

The FortiAuthenticator API can be used to integrate third party User Identity Management Systems with FortiAuthenticator and ultimately FortiGate. The method will be summarized here but for the most up to date detail, see the FortiAuthenticator REST API Solution Guide http://docs.fortinet.com/fortiauthenticator/.

Pseudo code is provided that should allow a programmer to replicate in their chosen language.

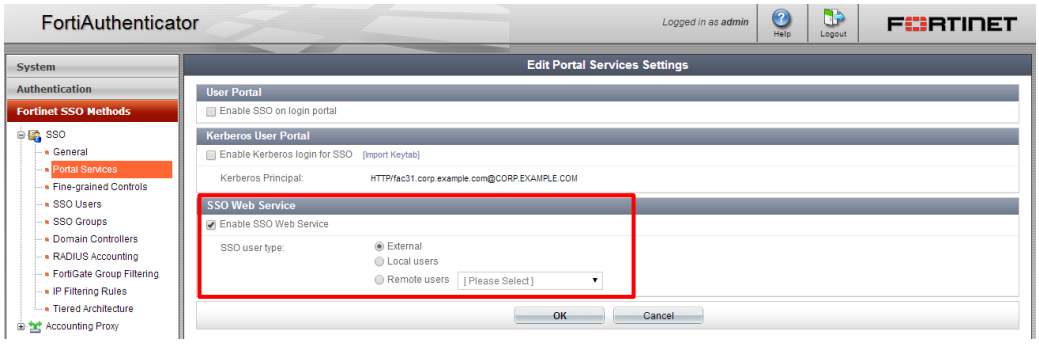
## Create a Web Service Key

Acquire a web services access key by creating an administrator account and enabling Web Service Access. The key will be emailed to the users email address specified in the User Information section.




## Enable the Web Service SSO Portal

Browse to *Fortinet SSO Methods* > *Portal Services* > *SSO Web Service* and ***Select*** *Enable SSO Web Service*.




Select the appropriate SSO User Type that will be accepted via the portal:

**External:** Users are derived from external source (e.g. RADIUS). Use this method when Username, IP and all relevant group info is defined in the RADIUS packet.

**Local Users:** User and IP info is contained in the RADIUS packet but user is defined locally and additional group info can be sourced from the local group database.

**Remote Users:** User and IP info is contained in the RADIUS packet but user is defined remotely and additional group info can be sourced from the LDAP.

## Using the Web Service SSO Portal

To (de)authenticate a user in FSSO it is possible to POST in XML or JSON format to the FortiAuthenticator REST API SSO Auth endpoint.

**URL:** https://[server_name]/api/[api_version]/ssoauth/

This API is for use by third party authentication systems for dynamic transparent user Single Sign-on to a Fortinet protected network. The following fields are supported on this endpoint.

| Field | Display Name | Type | Required | |
|---|---|---|---|---|
| event | Event type | integer/string | Yes | 0=Login<br>1=Logout |
| username | User's username | string | Yes | max length=253 |
| user_ip | User's workstation IP (Calling-Station-Id) | IPv4 | Yes | |
| user_groups | Groups to send (Fortinet-Group-Name) | string | No | max length=253, list of groups must be separated with "+" character (group name cannot contain a "+" character) |

## Example logon event

To authenticate (JSON format):

```
Username    = john.doe
IP          = 10.1.73.175
Group       = FW_Admins       (Optional)
```

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -d
'{"event":"0","username":"cwindsor","user_ip":"10.1.73.175",”user_
groups”:”FW_Admins”}' -H "Content-Type: application/json"
https://192.168.0.122/api/v1/ssoauth/
```

## Example logout event

To deauthenticate the same user (JSON format):

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -d
'{"event":"1","username":"cwindsor","user_ip":"10.1.73.175"}' -H
"Content-Type: application/json"
https://192.168.0.122/api/v1/ssoauth/
```

# Logout Detection

## WMI Workstation Verification

WMI based workstation verification is supported by a subset of the SSO methods.

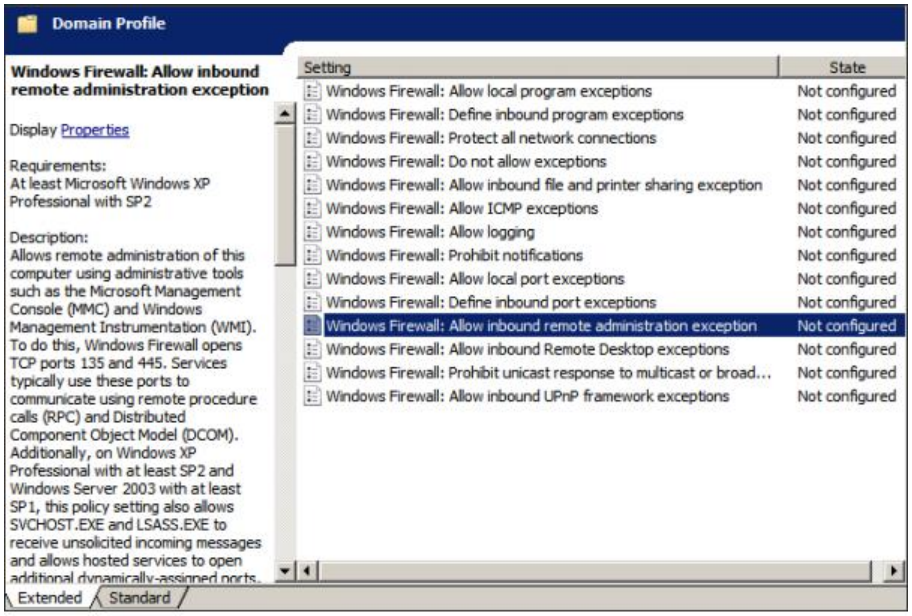
- Perform a reverse DNS lookup of the users workstation
  - If reverse DNS lookup successful, use the admin account of the DC as specified in (SSO>DomainControllers) that matches the workstation's domain
  - If reverse DNS lookup fails, or no DC matches the workstation's domain, use the admin account of the DC matching the user's domain.
- Use the gathered admin account to query WMI on the workstation to check current user

### Permissions required

WMI Polling relies on the ability of the FortiAuthenticator to reach the WMI process on the client workstation. Fire wall rules may prevent this and require the following to be enabled.

```
netsh firewall set service RemoteAdmin enable
```

A more specific exception can be made using group policy for multiople systems.




The administrator account used for WMI polling features utilizes the Windows Active Directory Domain Authentication permissions from Authentication > RemoteAuthServers > LDAP. For successful WMI polling, this user must have Remote Management Users permissions within the Windows Domain.

**To verify adequate permissions:**

Open the Windows Command Prompt and execute the following commands:

```
C:\WINDOWS>wmic
wmic:root\cli>/user: CORP\DomainAdmin
Enter the password :********

wmic:root\cli>/node: 192.168.1.150
wmic:root\cli>computersystem get username /value

UserName=CORP\atano

wmic:root\cli>
```

# FSSO Method Comparison and Deployment Scenarios

The best method of authentication to use in your environment is largely dependent on your environment e.g.

- Number of DCs
- Number of users (and authentications per second)
- Network architecture

The following table details what features are supported with each implementation method.

| | Mode | Agentless (Client) | Agentless (DC) | Transparent | No Additional Requirements | MAC Support | Logoff Detected | IP Change Detected | Scalability |
|---|---|---|---|---|---|---|---|---|---|
| FSSO Software | DC Agents | ✓ | ✗ | ✓ | ✗[1] | ✓ | ✓[2] | ✓[1] | High |
| | NTLM | ✓ | ✗ | ✗ | ✗[2] | ✗ | ✓[2] | ✓ | Med |
| | API Polling | ✓ | ✓ | ✓ | ✓ | ✗ | ✓[2] | ✗ | Low |
| | eDirectory | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | High |
| | WinSecLog Polling | ✓ | ✓ | ✓ | ✓ | ✓ | ✓[2] | ✗ | Med |
| FortiAuthenticator | WinSecLog Polling | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | Med-High |
| | FSSO Portal | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | High |
| | Portal Widgets | ✓ | ✓ | ✗ | ✗[4] | ✓ | ✓ manual | | High |
| | FortiClient SSO Mobility Agent | ✗ | ✓ | ✓ | ✓ | Roadmap | ✓ | ✓ | High |
| | RADIUS to FSSO | ✓ | ✓ | ✓ | ✗[5] | ✓[6] | ✓[6] | ✓[6] | High |

[1] Requires DNS to be updated with a machine name to IP address mapping

[2] Requires RPC port polling.

[3] Web browser must support NTLM, SSL Certificate warnings generated

[4] For optimal configuration, FortiAuthenticator Portal Widgets should be embedded in a user intranet page and this page set as their browser home page.

[5] Customer (usually carrier) RADIUS Server must be able to send accounting start packets to FortiAuthenticator containing the client IP address.

[6] Dependent on customer RADIUS / network implementation

## Deployment Scenario 1 – Medium Enterprise

A common enterprise deployment will consist of:

- Windows desktops
- Active directory infrastructure with a low number of domain controllers

For such a deployment, the recommended configuration of FortiAuthenticator would be to poll the domain controllers for logon events. Should a user roam on the wireless network for example, this may not trigger a login event so a fallback method of authenticating the user such as the FSSO Portal would help to cover such eventuality.

## Deployment Scenario 2 – Large Enterprise

Large enterprise deployments are similar to their medium enterprise counterparts but may include

- Higher number of windows desktops
- Larger number of domain controllers with forests and trust relationships
- Distributed network with possibility of high latency links

In this scenario, Domain Polling may not scale to the required level and distributed nature of the enterprise so other solutions should can also be considered. Given the fact that the Entrprise have control over the desktop operating system, the FortiClient SSO Mobility Agent can be rolled out to the organization via GPO. This allows for:

- Greater scalability
- Better support for geographically dispersed users
- Logoff detection
- IP roaming detection

Optionally this method can be combined with others such as the FSSO Portal to catch edge cases with unauthenticated devices and unsupported operating systems.

## Deployment Scenario 3 – University

There are several specifics about University deployments that makes them somewhat unique.

- Generally large number of endpoints
- Large estate of centrally managed Windows desktops (library open-access access clusters)

- Mix of other endpoint types (Linux, Solaris, Mac)
- BYOD common (guest wireless with iPad, iPhone, Android, various OS laptops)

For such a deployment, a combination of several FSSO methods can be used to cover all scenarios e.g.

- FortiClient SSO Mobility Agent for University owned Windows Desktops
- FSSO Portal with home page embedded widgets for personal or alternative OS devices

## Deployment Scenario 4 – Wireless network / Mobile carrier

Large scale wireless networks and mobile carriers have a commonality in the network architecture; their use of RADIUS as the authentication method. When a user authenticates on a network via RADIUS, it is possible to forward RADIUS accounting records to the FortiAuthenticator to use as a source of information regarding the identity of the user.

To use this method, there is a pre-requisite that the Accounting packets contains:

- Username (or some other piece of information that identifies the user such as MSISDN)
- Client IP Address
- Group information (optional as this can also be gathered via an LDAP lookup)

# Appendix A – Domain Account Permissions

| Feature | FortiAuthenticator Configuration Location | Minimum Windows Permissions |
|---|---|---|
| LDAP Authentication | Authentication > RemoteAuthServers >LDAP | **Domain Controller:** `Read` permission for specified domain |
| LDAP Group Queries | | `Read Member Of` for specified LDAP directory |
| Active Directory Polling<br>(Security Event Log) | Fortinet SSO Methods> SSO > Domain Controllers | `Event Log Readers` |
| WMI Workstation Verification | SSO->DomainControllers | `Remote Management Users`<br><br>Note that the local firewall must allow FortiAuthenticator connect to the required ports. |
| FAC Agent for Microsoft Windows | *Windows software* | **Install:** `Domain Admin`<br>**Config:** `Domain Admin`<br>**Use:** `Domain User` |
| SSO Mobility Agent | *Windows software* | **Install:** `Domain Admin`<br>**Config:** `Domain Admin`<br>**Use:** `Domain User` |

# Appendix B – FSSO Methods

| Method | Authentication Endpoint | User Experience | Agent Required | Logoff |
|---|---|---|---|---|
| Windows Active Directory Polling | Windows Domain | Transparent | No | WMI |
| Kerberos | Windows Domain | Transparent | No | Timeout |
| Single Sign On Mobility Agent | Windows Domain | Transparent | Yes | *Yes* |
| Login Portal | Any | Manual | No | Timeout / Manual |
| Embedded widget | Any | Initial manual authentication then transparent | No | Timeout / Manual |
| REST API | Portals and third party applications | Transparent * | No | Yes |
| DC Agent | Windows Domain | Transparent | Yes | Timeout |
| TS Agent | Citrix/Windows Terminal Server | Transparent | Yes | Timeout |
| RADIUS Accounting | Commonly Wireless controllers. SSL VPN, third party RADIUS systems | Transparent | No | Yes |

# Appendix C – Debugging RADIUS Accounting

To test RADIUS Accounting and verify correct configuration, it is most simple initially to test with desktop tools siuch as NTRADPing (provided by http://www.mastersoft-group.com/download/).

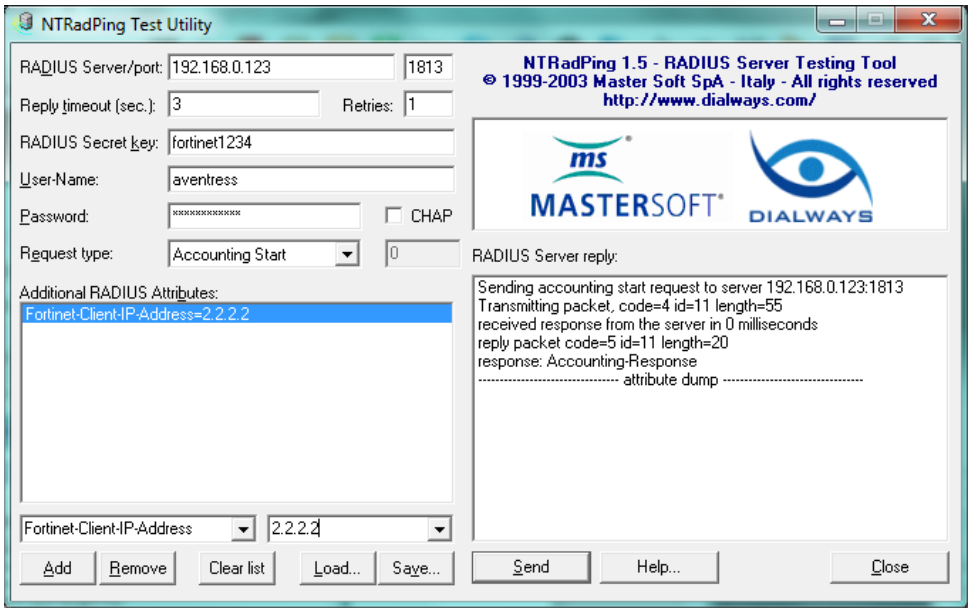
Once downloaded and installed, follow the instruction to install the Fortinet RADIUS Dictionary into the application.

To trigger a login into FSSO, the RADIUS packet must contain

User-Name = <User name>

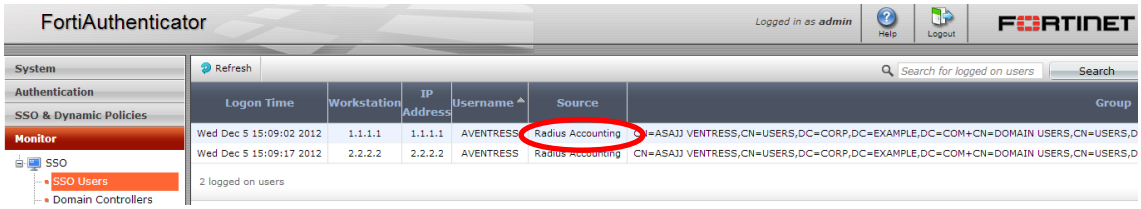
Fortinet-Client-IP-Address = <Client IP>

To replicate sending of these attributes configure the NTRADPing software as shown:




- Take care to ensure the *RADIUS Port* is changed to ***1813*** and the *Request type* is set to ***Accounting Start.***
- If successful, FortiAuthenticator will acknowledge the receipt of the packet and the NTRADPing client will display this success with *"Accounting-Response".*
- If this is not successful, verify that UDP1813 can pass to the FortiAuthenticator and that the RADIUS Secret Key is configured correctly on both sides.

A successful RADIUS → FSSO authentication will result in a "RADIUS Accounting" Logon event being displayed in the authentication monitor and being passed to the FortiGate.




If an authentication is not shown, check the RADIUS debugging logs https://<FAC_IP/debug/radius/. Authentication may be successful but the user not found in LDAP (or LDAP is not configured correctly). In this case the login will be received but the record dropped due to lack of group info.

# Appendix D – RADIUS Dictionary

```
#############################################################
#
#
# Fortinet, Inc. #
#
#
# RADIUS VSA Dictionary #
#
#
# This RADIUS dictionary is to be used in conjunction #
# with FortiOS v4.0.0. #
#
#
# Copyright 2009 #
#
#
# Technical Support
#
# http://www.fortinet.com/support #
#
#
#############################################################
VENDOR Fortinet 12356
BEGIN-VENDOR Fortinet
ATTRIBUTE Fortinet-Group-Name 1 string
ATTRIBUTE Fortinet-Client-IP-Address 2 ipaddr
ATTRIBUTE Fortinet-Vdom-Name 3 string
ATTRIBUTE Fortinet-Client-IPv6-Address 4 octets
ATTRIBUTE Fortinet-Interface-Name 5 string
ATTRIBUTE Fortinet-Access-Profile 6 string
#
# Integer Translations
#
END-VENDOR Fortinet
```